Bugzilla ID: 378882
Bugzilla Summary: Add Deutsche Telekom CA cert for T-system Trust Center

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.

General Information	Data
CA Name	**T-Systems**
Website URL (English version)	http://pki.telesec.de/service/certificates/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.)	T-Systems is a wholly-owned subsidiary of Deutsche Telekom AG.
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?)	T-Systems is part of Deutsche Telekom Group, which means that we have more than 50 million customers worldwide and about 160.000 business customers that receive ICT services from us. Being able to provide secure and convenient services to our customers on the Mozilla platform would help not only us but also Mozilla on its goal to address the business market as well.

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	Deutsche Telekom Root CA 2	COMPLETE
Cert summary / comments	Operated at the T-Systems Trust Center	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://wwwca.telesec.de/cgi-bin/caservice/Common/InstallRoot/DT-Root-CA-2.cer	COMPLETE
SHA-1 fingerprint.	85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF	COMPLETE
Valid from	1999-07-09	COMPLETE
Valid to	2019-07-09	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	2048	COMPLETE

CRL • URL • update frequency for end-entity certificates	http://pki.telesec.de/cgi-bin/service/af_DownloadARL.crl?-crl_format=X_509?-issuer=DT_ROOT_CA_2 Find below a translated extract of the CPS of DT CA 2: "4.9.7 Frequency of the publishing from revoked information (CRL) The CRL will we published and offered in standardised form every 6 months. If there is a relevant revoking related this CRL within these 6 months, it will generate a new CRL to this event. 4.9.8 Maximum latency of the revocation lists the latency of the revocation list is at least 12 hours." For **end entities** please see e.g. CPS of T-TeleSec MailPass Advanced: "2.3.5 Publishing of Certification Revocation List The CRL is generated and published **at least every 24h.** The crl is generated with a latency of 4h."	COMPLETE At least every 24 hours
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation EV Guidelines section 26(a): "OCSP responses from this service MUST have a maximum expiration time of ten days."	None	COMPLETE
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate 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.	The CA issues certs for Sub CAs that issue certificates for SSL enabled servers, signed and encrypted emails and documents and digitally signed executable code CPS: "Each certification authority has one or more CA(s) and service certificates issued by the relevant higher-level root CA that are re-issued in regular intervals. The certification authorities for advanced certificates shown above and operated by T-Systems or other operators are governed by the T-Systems CP."	COMPLETE

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. (For example, contractual arrangements should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	Olaf: I only know one of the subordinate CAs, so: Yes, subordinate CAs exist. In the CPS of the Deutsche Telekom, section 1.3.1.1 states that the subordinate CAs have to follow the CP of the Deutsche Telekom. Comment #37 states that contracts and audits are in place... CPS: The T-Systems Trust Center operates the "Deutsche Telekom Root CA 2" root CA for advanced certification services. The root CA certificate is a self-signed certificate and is published by T-Systems. … The certification authorities for advanced certificates shown above and operated by T-Systems or other operators are governed by the T-Systems CP. Comment #37: To answer that question: We do not give certificates to private (single) persons with one exception: certificates for qualified signatures according to the German Signature Act. Those certificates contain no email addresses or domain information, so there is no prove required for those data. All other certicates are being issued to **enterprise customers (we provide CA functions as a managed service or dedicated PKI environments that comply to our policies**) In both cases the customer has to prove as a minimum that 1. **he owns the domain** 2. complies to our CPs (by signing a contract and the assured readiness to allow audits whenever we consider them necessary)(audits for customer location are being performed before dedicated PKI Environments can go live) 3. his internal processes ensure a proper mapping of employees and enterprise identities as part of the RA function (by providing documents and allowing audits). Comment #52: The CA currently has 2 subordinate CAs that are operated by third parties, oneof them serving the community of the the German Research Network (Deutsches Forschungsnetz, DFN). There are certainly contractual obligations to meet at least the standard of the CP of the Root. Those	COMPLETE

	contracts include the right to perform audits on the subordinate Ca (with full on-site access). Those audits are performed regularly (once a year) or on purpose (See chapter 8: Audits and other assessment criteria). Those rules will apply to all other possible future SubCAs as well.	
List any other root CAs that have issued cross-signing certificates for this root CA	None as per hierarchy diagram in the CPS: "The root CA only certifies certificates from direct subordinate certification authorities."	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLETE
If SSL certificates are issued 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. (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.)	DV, IV/OV Comment #37: All other certificates are being issued to **enterprise customers (we provide CA functions as a managed service or dedicated PKI environments that comply to our policies**) In both cases the customer has to prove as a minimum that 1. **he owns the domain** … CPS: The basic requirement for a new order is an existing contractual relationship. This contractual relationship is generated by T-Systems sales units with help from the legal departments. **This ensures sufficient authentication of the external customer.** The CPS says: "Unverified end subscriber information is information that is included in the certificate without being checked and includes:. the organizational unit (OrgU)" Comment #47: OU (= organizational unit) entries are not O (= organization) entries. Usually OU entries are just the names of internal departments or working groups (which usually cannot be validated by anyone outside the company anyways). Comment #52:	COMPLETE

	OU (= organizational unit) entries are not O (= organization) entries. Usually OU entries are just the names of internal departments or working groups (which usually can't be validated by anyone outside the company anyway). So we bind the domain to the Organisation, not to OUs that change all the time in modern enterprises. Checking, whether OUs are valid or not comes down to the same problem as with E-Mail. We do check, whether there is a process in place to assign the right data to people who are going to receive certificates in an enterprise(automized data collection and manual checking by the RAs in place), but how this is being done in detail is always described in the CPS of the SubCA, that issues EE certificates.	
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	N/A	N/A
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 example.	https://www.pki.dfn.de/	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	http://pki.telesec.de/service/DT_ROOT_CA_2/T-Systems-Root-CP-deutsch-v11.pdf http://pki.telesec.de/service/DT_ROOT_CA_2/cps.pdf English: http://pki.telesec.de/service/documents/T-Systems-CPS-CA-2-English-v11.pdf http://pki.telesec.de/service/documents/T-Systems-Root-CP-English-v12.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.)	WebTrust Ernst and Young : http://www.de.ey.com Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=701 https://cert.webtrust.org/SealFile?seal=701&file=pdf	COMPLETE

After Info Gathered: (I couldn't find this info in the CPS, but it appears to be **handled in the contractual agreements with enterprise customers** who each own a subordinate CA to this root, and only issue end-entity certs within their organizations, see Comment #37. So these checks would be the responsibility of the enterprise, and would be in the CPS for each enterprise customer.)
Review CPS sections dealing with subscriber verification

- Verify domain check for SSL
    - Comment #52: Section 3.2 of the CP describes the evaluation of involved parties. DT Root CA 2 is being used for Enterprise Services exclusively, which means that DT Root CA 2 issues no EE certs but certs for subCA's of enterprise customers that have decicated PKI or use our "PKI as a service". Those enterprise customers are contractually bound to comply with our rules or have no choice to do otherwise in case they receive our PKI services. Checking for the ownership of the domain is part of the legal process to come to a contract with those customers (It`s no big deal to examine the ownership of the domain via the responsible NIC).
- 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.
    - Olaf, Comment #47: "Yes, end-entity email-certificates exist. Again I cannot answer this for all Telekom customers. In the German Research Network, personal identification of each user and validation of email address is required (and it's in the CP of the DFN). The Telekom CP and CPS are not clear on this point (as far as I have seen)."
    - Comment #52: OU (= organizational unit) entries are not O (= organization) entries. Usually OU entries are just the names of internal departments or working groups (which usually can't be validated by anyone outside the company anyway). So we bind the domain to the Organisation, not to OUs that change all the time in modern enterprises. Checking, whether OUs are valid or not comes down to the same problem as with E-Mail. We do check, whether there is a process in place to assign the right data to people who are going to receive certificates in an enterprise(automized data collection and manual checking by the RAs in place), but how this is being done in detail is always described in the CPS of the SubCA, that issues EE certificates.
- Verify identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)

Comment #37 in bugzilla:
"Gerv used to ask all other requestors about their verification process for email certificates (How they verify that the requestor owns the email address).

To answer that question**: We do not give certificates to private (single) persons with one exception: certificates for qualified signatures according to the German Signature Act. Those certificates contain no email addresses or domain information, so there is no prove required for those data.**

All other certicates are being issued to enterprise customers (we provide CA functions as a managed service or dedicated PKI environments that comply to our policies) In both cases the customer has to prove as a minimum that

1. he owns the domain
2. complies to our CPs (by signing a contract and the assured readiness to allow audits whenever we consider them necessary)(audits for customer location are being performed before dedicated PKI Environments can go live)
3. his internal processes ensure a proper mapping of employees and enterprise identities as part of the RA function (by providing documents and allowing audits).

We consider this to be sufficient to prevent people from impersonating others. (At least nobody should be able to request successfully a certificate for bill.gates@microsoft.com or george.bush@whitehouse.gov). Still there can't be no absolute certainty within enterprise domains, since typically to many systems and people have access to the IT based identity and ressources of employees)
"

Flag Problematic Practices (complete)

- Long-Lived Domain-Validated SSL certs (not found)
- Wildcard DV SSL certs (not found)
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA (no)
- Allowing external entities to operate subordinate CAs
    - Yes, see table above.

Verify Audits (complete)

- Validate contact info in report, call to verify that they did indeed issue this report.
- For EV CA's, verify current WebTrust EV Audit done.
- Review Audit to flag any issues noted in the report