Bugzilla ID: 892390
Bugzilla Summary: Add T-Systems Root CA Certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	T-Systems International GmbH
Website URL	http://www.telesec.de , http://www.t-systems.com
Organizational type	Commercial Company: T-Systems International GmbH is a German limited liability company and a wholly owned subsidiary of Deutsche Telekom AG.
Primark Market / Customer Base	T-Systems is part of Deutsche Telekom Group, which is serving more than 50 million customers worldwide and about 160.000 business customers. T-Systems Trust Center is the organizational unit issuing certificates to our customers. Our focus is mainly Western Europe, especially Germany, but there are some international customers as well. We are providing services both to our business and consumer customers as well.
Impact to Mozilla Users	Among others we are issuing certificates to enterprises using S/MIME certificates for their employees, academic institutes for internal and external web services as well as email certificates for employees and students, airlines using SSL server certificates for their website and departments of Deutsche Telekom as internal customers. Relying parties can be the public consumer market as well as internal enterprise employees.
Inclusion in other major browsers	Opera, Oracle (Java), Microsoft, RIM Blackberry
CA Contact Information	CA Email Alias: telesec_support@t-systems.com CA Phone Number: +49 1805 268 204 Title / Department: Trust Center Services

Technical information about each root certificate

Certificate Name	T-TeleSec GlobalRoot Class 2
Certificate Issuer Field	CN = T-TeleSec GlobalRoot Class 2 OU = T-Systems Trust Center O = T-Systems Enterprise Services GmbH C = DE
Certificate Summary	This new SHA-256 root certificate will eventually replace the "Deutsche Telekom Root CA 2" root certificate that was included via Bugzilla Bug #378882. The old root has externally-operated subordinate CAs that will eventually be migrated to this new root.
Root Cert URL	http://www.telesec.de/downloads/GlobalRoot_Class_2.cer
SHA1 Fingerprint	59:0D:2D:7D:88:4F:40:2E:61:7E:A5:62:32:17:65:CF:17:D8:94:E9

Valid From	2008-10-01
Valid To	2033-10-01
Certificate Version	3
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	2048
Test Website URL (SSL)	https://root-class2.test.telesec.de
CRL URL	http://pki.telesec.de/rl/GlobalRoot_Class_2.crl http://crl.serverpass.telesec.de/rl/GlobalCA_Class_2.crl (NextUpdate: 24 hours) ServerPass CP/CPS section 4.9.7: …of end entities, is updated once a day and published by the repository.
OCSP URL	http://ocsp.telesec.de/ocspr http://ocsp.serverpass.telesec.de/ocspr CPS section 4.9.9: T-Systems maintenance a OCSP responder signed by the Root-CA to validate issued Sub-CA certificates. OCSP responses are valid for three (3) days. The OCSP repository is updated within 24 hours in cases a certificate is revoked. Sub-CA Requirements: Sub-CAs must maintain an OCSP responder to validate issued certificates. OCSP responses must have a maximum expiration time of ten (10) days. The OCSP repository must be updated at least every four (4) days.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV
EV Policy OID(s)	Not applicable. Not requesting EV treatment for this root.
Non-sequential serial numbers and entropy in cert	SP and SBCA: 7.1 Unique value used to identify the certificate. The certificate serial numbers are generated as 8-byte random values (entropy).

CA Hierarchy information for each root certificate

CA Hierarchy	CA Hierarchy Diagram is provided in section 1.3.1 of the CPS: T-Systems issues CA certificates for its own products and services as well as for other operators. … All certification authorities shown above and operated by T-Systems or other operators are governed by the CP of "T-TeleSec GlobalRoot Class 2".
Externally Operated SubCAs	Currently none, but there is one externally-operated subordinate CA that will eventually be migrated from "Deutsche Telekom Root CA 2" (legacy root) to "T-TeleSec GlobalRoot Class 2". -> The DFN subordinate CA serves the community of the German Research Network (Deutsches Forschungsnetz, DFN). DFN has a separate ETSI-Audit and operates a sub-CA for the Global security level certificates that are described in their CP. CA:SubordinateCA checklist:Third-Party Public Subordinate CAs -> DFN subordinate CA 1. Sub-CA name: DFN, Deutsches Forschungsnetz e.V. 2. Sub-CA URL: https://www.dfn.de 3. Sub-CA cert: https://www.pki.dfn.de/root/globalroot/ 4. CA hierarchy: http://www.telesec.de/pki/intermediate.html

	5. https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP.pdf https://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CPS.pdf 6. Sub-CA subscriber cert verification procedures: CP (section 3.2.2 and 3.2.3) 3.2.2 Authentication of an Organization Every organization that subscribes to DFN-PKI services has an existing contract for DFNInternet services with DFN-Verein. Before signing the contract, all information provided by the organization is validated against suitable documentation. Alternatively, organizations are being authenticated by validating suitable documentation such as certificates of registrations with the register of commerce and associations or by federal or state law or by presentation of letters of accreditation (issued by lawyers, notaries, chartered accountants or governmental institutions). Digital certificates are only being issued for the organizations' names stated by the contract or the presented documents. If a domain name is used in a certificate, the authorization of the organization to use this domain name is verified by DFN-Verein as operator of the DFN-PCA. These validations are repeated no later than 39 months. Certificates with a validity time of more than 39 months are revalidated after this period. All data used for revalidation must likewise not be older than 39 months. 3.2.3 Authentication of a Natural Person Authentication of the identity of a natural person is carried out by DFN-PCA. It can make use of suitable contractors for this task (e.g. PostIdent). The authentication is carried out by personal identity vetting using an official and valid photo-ID document (ID card or passport) and it is appropriately documented. The following information must to be available and must be verified: Name, first name(s) and name affixes as stated by identification document E-mail address Type and last five digits of the serial number of the identification document Name and address of the corresponding organization Proof of affiliation with the stated organization This information is mandatory for the issuance of certificates and documented. The data allows for the unambiguous identification of a natural person. 7. OV 8. No potentially problematic practices known. 9. DFN is audited annually by TUVIT according to the ETSI 102042 V2.2.1 criteria https://www.tuvit.de/data/content_data/tuevit_de/6727UD_s.pdf (2012.12.03) 10. The CRL update frequency for end-entity certificates is 24 hours (CP section 4.9.7 – still 72 hours – is not up to date and is corrected in the next version). 11. Test websites: https://info.pca.dfn.de/ (valid certificate with OCSP) https://revoked-demo.pca.dfn.de (revoked certificate with OCSP)
Cross-Signing	The currently included "Deutsche Telekom Root CA 2" root certificate has cross-signed with this new "T-TeleSec GlobalRoot Class 2" root certificate.

Technical Constraints on Third-party Issuers	ServerPass (SP): no Third-party-issuers Shared Business-CA (SBCA): external RA/Enterprise RA are technically restricted, to conduct domain verification and - if necessary- power of authority verification. Shared-Business-CA (subsequently referred SBCA) is a multi-tenant capable PKI-service for business customers. The name of the mandator is based on the domain name (e.g. example.com, see CP/CPS section 3.2.2). The existence of the customer is checked by a recent official public document (e.g. certificate of registration or equivalent). Furthermore, the domain is checked against a WhoIs database. The mandator may have issued different types of certificates by the CA (e.g. user, server). Among other things, the certificate content contains a mail address or DNS-name. The mandator´s-config-parameter "allowed internet domains" for each type of certificate represent the technical restriction of the mandator. The "Domain Part" is checked for mail addresses, "First- and Second-Level-Domain" (if necessary Third- and Fourth-Level) for DNS-Names. In case the applicant is not owner of the domain, a power of authority is required in addition. Only verified and proven "allowed domains" T-Systems was included in the PKI configuration of the mandator, this means that the mandator can issue certificates to these domains. The domains will be reviewed within 39 months. The existence of mail addresses will be checked by challenge-response method. A web application with smartcard authentication is used for the mandator´s management. Each mandator can issue unique certificates only for the proven "allowed internet domains".

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.telesec.de/pki/roots.html CP (English): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cp_en.pdf CP (German): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cp.pdf CPS (German): http://telesec.de/pki/service/GlobalRoot_Class_2/CPS_T-TeleSec_GlobalRoot_Class_2_DE_V2.0.pdf ServerPass CPS (German): http://telesec.de/serverpass/cps.html (version 2.0, July 2013) ServerPass CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=555341 (version 1.1, Dec 2010) Shared-Business-CA CPS (German): http://telesec.de/sbca/cps.html (version 2.0, July2013) Relying Party Agreement: Further details are described on base of dedicated "products" offered to customers. Please find below the link to the standard business conditions for one of our products as example / this is available in german only: http://www.telekom.de/dlp/agb/pdf/41157.pdf
Audits	Audit Type: WebTrust for CA Auditor: Ernst & Young GmbH Auditor Website: http://www.ey.com/DE/de/Home/Home WebTrust for CA Audit Report: https://cert.webtrust.org/SealFile?seal=1531&file=pdf (2013.07.11) BR Audit Report: http://telesec.de/downloads/TSI13WebTrust-RootCAs_BaselineReport_final.pdf
Baseline Requirements (SSL)	Shared-Business-CA CPS section 1.1.2 translation: The Trust Center at T-Systems ensures that the root CA "German Telekom Root CA 2" and "T-TeleSec GlobalRoot Class 2" with the respective subordinate sub-CAs the requirements and regulations of the current published version of the [CAB must comply and follow-BR]

	(http://www.cabforum.org/documents.html). In the event of any inconsistency between this document and the [CAB-BR], the provisions of the [CAB-BR] take precedence. ServerPass CPS section 1.1.1 translation: The Trust Center at T-Systems to ensure that the sub-CAs for TeleSec ServerPass using the Requirements and regulations of the current published version of the [CAB-BR] (http://www.cabforum.org/documents.html) fulfills and complies. In case of conflict between the this document and the [CAB-BR], the provisions of the [CAB-BR] take precedence.
Organization Verification Procedures	Translation of section 3.2.2 (Authenticating the identity of organizations) and 3.2.3 (Authenticating the identity of end users) of the Shared-Business-CA CPS is attached to the bug. https://bug892390.bugzilla.mozilla.org/attachment.cgi?id=801757 ServerPass CPS section 3.2.2 Authentication of an organization TeleSec ServerPass Standard: The initial request can only be placed after successful registration in the customer portal <myServerPass>. In order to confirm the legal person named in the Subject Distinguished Name (subjectDN) of the certificate under Organization (O), the following document is required according to the business category: Legal person: The request form signed by an authorized signatory. Authority: The request form signed by an authorized representative of the authority and stamped with the official seal. Association: The certified copy (no more than 30 days old) of the register of associations excerpt must be submitted together with the signed request form. Trader(s): The certified copy (no more than 30 days old) of a current trade license and the personal ID of the trader must be submitted together with the signed request form. The following is checked for all business categories: - Is the information on the request form identical to the information in the Certificate Signing Request (CSR) of the online request? - Does the company name of the organization/company correspond to the entry in the electronic commercial register or comparable directories (eg according to the foreign jurisdiction, the Register of Associations) match? Do current organization documents (no more than 30 days old) issued by a competent authority also confirm the organization's existence (e.g., register of associations or comparable document, official stamp)? - The address of the organization is measured by the electronic Commercial register or similar directories. The applicant must operate a branch, office or similar at the specified location, - The authorization of the responsible contact at the organization named in the request (legal person), - If a third party carries out the certificate request/management on behalf of the organization, it must have a corresponding written authorization concerning the transfer of rights Additionally or alternatively the existence or the address of the organization will be verified to the commercial register or similar directories, other methods are used. If necessary, a Dun & Bradstreet report can be used as a trusted, reliable and independent data source.

	An attorney from an appropriately qualified person is also allowed. Similarly, an employee of the certification body or a authorized third party confirm the specified location in person.
SSL Verification Procedures	According to the ServerPass CPS section 3.2.2, T-Systems verifies the organization, the authority of the certificate subscriber to request the certificate, and that the customer owns the domain or has been given the exclusive right to use the domain to be included in the certificate. Official directories and Whois are checked ServerPass CPS section 3.2.5.2, Examinations of domains and ip-addresses The T-Systems registration authority employee checks for each of the SAN-entries (FQDN or ip-address) whether the applicant has the legitimate right to use the relevant domain or ip-address. This involves querying the online database of the country-specific NIC unit (e.g., Denic eG for Germany) for geographic ccTLDs or the online database of the WhoIs for gTLDs. To check an IP address, adequate online databases are queried. If this does not lead to a successful result, it is checked whether the applicant has been authorized through a power of attorney by the domainowner to use the domain or IP address. The power of attorney must be signed by an authorized person or by the person who signed the contract with T-Systems International GmbH. Translations of the following sections of the Shared-Business-CA CPS have been attached to the bug https://bug892390.bugzilla.mozilla.org/attachment.cgi?id=801757 3.2.5.1 – Ensuring the authenticity of the certification request 3.2.5.2 – Checking domains and IP addresses "The customer notifies T-Systems of the domains for which certificates are to be issued so that T-Systems can check them, include them in the client's PKI configuration as "permitted Internet domains" and maintain them. … The T-Systems registration authority employee checks for each entry whether the customer (client) has the legitimate right to use the relevant domain. This involves querying the online database of the country-specific NIC unit (e.g., Denic eG for Germany) for geographic ccTLDs or the online database of the WhoIs for gTLDs. To check an IP address, adequate online databases are queried." 3.2.5.3 – Additional checks by the client 4.2.1.2 – External registration authority "If the certificate is requested electronically via the relevant website or e-mail interface, the domain part of the e-mail address (optionally also the UPN) is checked for the "permitted Internet domains" entered in the PKI configuration. In the case of device certificates, the domain part of the e-mail address or the DNS name (top level domain and other FQDN sub-domains) is to be checked for the "permitted Internet domains" entered in the PKI configuration, depending on the certificate type."
Email Address Verification Procedures	SBCA CP/CPS (http://telesec.de/sbca/cps.html): 4.2.1 Performing identification and authentication functions -> 4.2.1.2 External Registration authority (RA) - The external Registration authority (RA) has to verify the mail-address for EE certificates used for Mail-Security (S/MIME-certificates) - issued by Sub-CA "Shared Business CA 3" or "TeleSec Business CA 1"- using a challenge response procedure where the end user is requested proactively to verify the existence of the e-mail address.

Code Signing Subscriber Verification Procedures	Not applicable. Not requesting the code signing trust bit at this time.
Multi-factor Authentication	ServerPass and Shared-Business-CA CPS section 6.5.1.1: Workplaces for certificate issuance are restricted by multi-factor authentication.
Network Security	In September 2012, the international auditing company Ernst & Young audited T-Systems' IT Basic Infrastructure Services with the Independent Service Auditors Assurance Report (ISAE 3402 Type II Report). This annual report is for internal use only. Upcoming, the Network and Certificate System Security Requirements will be incorporated into the WebTrust Service Principles and Criteria for Certification Authorities, see Audits.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes. See above.
CA Hierarchy	Yes. See above.
Audit Criteria	Yes. See above.
Document Handling of IDNs in CP/CPS	Not applicable.
Revocation of Compromised Certificates	CPS section 4.9
Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Yes. See above.
Verifying Identity of Code Signing Certificate Subscriber	Not applicable.
DNS names go in SAN	The DNS name is transferred to the SAN field.
Domain owned by a Natural Person	There will be no SLL certificates issued for domains owned by natural persons.
OCSP	Yes. See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV.
Wildcard DV SSL certificates	SSL certs are OV.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	SP: There is no externally-operated Sub-CAs or RAs. **SBCA: Yes. See above.**
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	**Yes. See above.** For external entities operating subordinate CAs we will enforce undergoing valid Webtrust or ETSI certification. We will amend the requirements for subordinate CAs in "T-Systems RootSigning" document.
Distributing generated private keys in PKCS#12 files	T-Systems Trust Center is NOT generating private keys for EE certificates
Certificates referencing hostnames or private IP addresses	Only FQDN or IP addresses, which can be resolved by DNS are used

Issuing SSL Certificates for Internal Domains	T-Systems Trust Center has followed the recommended "internal" audit and there were no issues found. RA employees are aware of the issue. The topic is discussed during the regular scheduled trainings. Validation procedures for .int domains are the same as for all other TLD.
OCSP Responses signed by a certificate under a different root	OCSP works without error in Firefox.
CRL with critical CIDP Extension	CRLs imported without error in Firefox.
Generic names for CAs	CN has T-TeleSec, and O has T-Systems
Lack of Communication With End Users	CPS is including contact details for any question or comment. This is not limited to entities or people having any kind of contract with T-Systems.