Bugzilla ID: [**xxx**](https://bugzilla.mozilla.org/show_bug.cgi?id=669849)

**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>.
3. Review the Recommended Practices at <https://wiki.mozilla.org/CA:Recommended_Practices>
4. 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. |
| Primary 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 | Mozilla’s Firefox is the most commonly used web browser in Germany having a market share of nearly 50%. 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 and consumer market as well  T-Systems Trust Center is maintaining a couple of root certificates and appropriate SubCAs. Looking at all those SubCAs we are issuing all of the following types of EE certificates (but not all are provided by each of the SubCAs):  - Websites (SSL/TLS)  - Email (S/MIME)  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.  Therefore relying parties can be the public consumer market as well as internal enterprise employees. |
| Inclusion in other major browsers | Opera, Oracle (Java), RIM Blackberry |
| CA Contact Information | CA Email Alias: [telesec\_support@t-systems.com](mailto: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 | Root certificate “**T-TeleSec GlobalRoot Class 2**” is intended to replace the already included root certificate  “**Deutsche Telekom Root CA 2**” in a long term run.  TeleSec ServerPass (SP) issuing ssl certificates for webserver and client authentication, cps 🡪 <http://telesec.de/serverpass/cps.html>  TeleSec Shared Business CA (SBCA) issuing email, ssl certificates for webserver and client authentication, VPN certificates for gateway and client authentication, Smartcard-LogOn 🡪 <http://telesec.de/sbca/cps.html>  Please feel free noting our adequately request for root embedding:  In July, 2011, we started the Mozilla Root Program to include our root “**T-TeleSec GlobalRoot Class 3 (EV)**” (see Bugzilla-ID: 760313 and 669849 - Target Milestone: Firefox 23). |
| 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)  Example Certificate (non-SSL) | <https://root-class2.test.telesec.de> |
| CRL URL | <http://pki.telesec.de/rl/GlobalRoot_Class_2.crl>  **Service TeleSec ServerPass for ssl/tls authentication:**  <http://pki.telesec.de/rl/GlobalCA_Class_2.crl>  Extract of ServerPass CP/CPS  4.9.7 Frequency of publication of revocation information  [ … ]  The certificate revocation list (CRL), which contains the revoked certificates of end entities, is updated once a day and published by the repository.  **Service TeleSec Shared Business CA for Email(S/MIME) certificates:**  http://crl.sbca.telesec.de/rl/GlobalRoot\_Class\_2.crl  4.9.7 Frequency of publication of revocation information  [ … ]  The certificate revocation list (CRL), which contains the revoked certificates of end entities, is updated once a day and published by the repository. |
| OCSP URL | **TeleSec ServerPass:**  OCSP URI in EE Cert: <http://ocsp.telesec.de/ocspr>  OCSP URI in EV Intermediate Cert: <http://ocsp.serverpass.telesec.de/ocspr>  **TeleSec Shared Business CA**:  OCSP URI in EE Cert: <http://ocsp04.telesec.de/ocspr>  CPS:  4.9.9 Availability of online revocation/status information  Revocation information will be provided online for the certificate users (see Section 2.1) based on a procedure  that complies with the standard. All CA certificates revoked by this certification authority are included. Online  information on the certificate status is available via OCSP at http://ocsp.telesec.de/ocspr.  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) | N/A |
| 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**  “\* The **Deutsche Telekom Root CA 2** certificate currently has still only 2 subordinate CAs that are operated by third parties; one of  them serving the community of the German Research Network (Deutsches Forschungsnetz, DFN), and the other issuing  certificates internally to Fraunhofer Corporate PKI (FhG) employees and systems.  \*\* DFN with a separate ETSI-Audit operates a sub-CA of the Deutsche Telekom Root CA 2 certificate, for the Global security level certificates that are described in their CP.  \*\* FhG operates one sub-CAs that chain up to the Deutsche Telekom Root CA 2 certificate and issues end-entity  certificates for employees.”  “\* The FhG (externally-operated sub-CA) has one internally-operated subordinate CAs. The sub-CA provides certification  services to their own employees. All FhG employees are registered within their own SIGMA system.“  The two externally operated subordinate CAs will be migrated from “Deutsche Telekom Root CA 2” (legacy root) to “**T-TeleSec GlobalRoot Class 2**” in a long term run.  In detail, all running services will chain up to the “T-TeleSec GlobalRoot Class 2” because of the security level the next 3 to 5 years. |
| Cross-Signing | Root CA “Deutsche Telekom Root CA 2” root certificate which is currently included in NSS has cross-signed with this new “T-TeleSec GlobalRoot Class 2” root cert. |
| Technical Constraints on Third-party Issuers | SP: no Third-party-issuers  SBCA: external RA/Enterprise RA are technically restricted, to conduct domain verification and - if necessary- power of authority verification. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | 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>  CP/CPS TeleSec ServerPass (German): <http://telesec.de/serverpass/cps.html>  CP/CPS TeleSec Shared Business-CA (German): <http://telesec.de/sbca/cps.html>  **Relying Party Agreement:**  Further details are described on base of dedicated “products” offered to customers. Please find below the link to the [standard](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=standard&trestr=0x1001) [business](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=business&trestr=0x1001) [conditions](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=conditions&trestr=0x1001) 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=1385&file=pdf> (2012.07.21) |
| Baseline Requirements (SSL) | SP and SBCA: CPS (<http://telesec.de/serverpass/cps.html>, <http://telesec.de/sbca/cps.html>):  1.1.1: Adherence to the CA/Browser Forums Baseline Requirements  T-System’s Trust Center warrants that the Root CA „Deutsche Telekom Root CA 2“ and all sub CA issued beneath  conforms at all times to the current version of the Baseline Requirements for the Issuance and Management  of Publicly-Trusted Certificates ([CAB-BR]) published at http://www.cabforum.org/documents.html. In the  event of any inconsistency between this document and the [CAB-BR], the [CAB-BR] take precedence over this  document.  Sub CAs at any hierarchy level chaining to the Root CA „Deutsche Telekom Root CA 2“ shall publicly give effect  to the [CAB-BR] by representing an equivalent statement like to one above in its CP or CPS. |
| SSL Verification Procedures | From T-Systems: The domain validation is performed by using WHOIS information. The certification application can be  successfully validated if the domain owner shown by WHOIS is literally equal to the name listed in the certificate's  "Organization" (O) field.  This may not be the organization which submitted the certificate application. In this case an additional letter of attorney  stating that the applicant is acting on behalf of the domain owner is mandatory needed. The person signing the letter of  attorney itself must be either listed in an official register (e.g. Commercial Registry) or a person listed in the register  confirms by an second letter of attorney that the signing person is allowed to sign on behalf of the organization for this  subject matter.  SP and SBCA CPS (<http://telesec.de/serverpass/cps.html>, <http://telesec.de/sbca/cps.html>):  3.2.2 Authentication of an organization  [ …. ]  The following is checked for all business categories:  [ …. ]   * Does the domain name correspond to the official directories? Does the customer own the domain; i.e., has he been given the exclusive right of use by means of a corresponding authorization? * 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 * Are any necessary Whois entries available.   [ …. ]  3.2.4 Non-verified subscriber information  No non-verified subscriber information. |
| Organization Verification Procedures | SP CPS (<http://telesec.de/serverpass/cps.html>):  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? 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 authorization of the responsible contact at the organization named in the request (legal person), * Does the domain name correspond to the official directories? Does the customer own the domain; i.e., has he been given the exclusive right of use by means of a corresponding authorization? * 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 * Are any necessary Whois entries available. |
| 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 challenge response.   [ …. ] |
| Code Signing Subscriber Verification Procedures | N/A – Not requesting the code signing trust bit at this time. |
| Multi-factor Authentication | CPS - SP and SBCA: 6.5.1.1 System-Security  […]  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**](https://wiki.mozilla.org/CA:Recommended_Practices))

|  |  |
| --- | --- |
| Publicly Available CP and CPS | Both, CP and CPS for all Root CAs maintained by T-Systems are available on the following website:  <http://www.telesec.de/pki/roots.html> |
| CA Hierarchy | T-Systems TrustCenter will use a hierarchical structure for the PKI. As the Root CA is an offline CA, there will be dedicated intermediate CAs. Each of those intermediate CAs will not be “multihomed”, means there is exactly one Root CA assigned to each of them.  Only the Root CA certificates are requested to be included within Mozilla’s NSS.  Each of T-Systems Root CAs as well as each of the intermediate CAs have a dedicated CPS available. |
| Audit Criteria | WebTrust CA is performed annually. |
| Document Handling of IDNs in CP/CPS | N/A |
| Revocation of Compromised Certificates | SP and SBCA: Compromised certificates will be revoked by T-Systems Trust Center (see CPS chapter 4.9 “Certificate Revocation and Suspension”. |
| Verifying Domain Name Ownership | See above. |
| Verifying Email Address Control | See above. |
| Verifying Identity of Code Signing Certificate Subscriber | See above. |
| DNS names go in SAN | N/A |
| Domain owned by a Natural Person | N/A, as there will be no SLL certificates issued for domains owned by natural persons. |
| OCSP | T-Systems Trust Center is providing OCSP service all owned CAs and EE certificates (see CPS).  All certificates will have to include the URI for the OCSP responder:  CA: <http://ocsp.telesec.de/ocspr>  EE: <http://ocsp.serverpass.telesec.de/ocspr> |

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

|  |  |
| --- | --- |
| Long-lived DV certificates | N/A – SSL certs are OV |
| Wildcard DV SSL certificates | N/A – SSL certs are OV |
| Email Address Prefixes for DV Certs | N/A – SSL certs are OV |
| Delegation of Domain / Email validation to third parties | SP: There is no externally-operated Sub-CAs or RAs.  SBCA see: Email Address Verification Procedures (Mail-Security) |
| Issuing end entity certificates directly from roots | N/A, root CA will NEVER issue EE certificates |
| Allowing external entities to operate subordinate CAs | 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 | N/A, as T-Systems Trust Center is NOT generating private keys for EE certificates |
| Certificates referencing hostnames or private IP addresses | N/A, as 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 procedure for .int domains are the same as for all other TLD. |
| OCSP Responses signed by a certificate under a different root | N/A, OCSP responses are always signed by the CA which issued the revoked certificate |
| CRL with critical CIDP Extension | N/A, as no “partitioned” CRLs are used |
| Generic names for CAs | N/A – CN and O fields in issuer are clear. |
| 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. |