**Bugzilla ID:** 669849
**Bugzilla Summary:** Add T-Systems Root CA Certificate and enable it for EV

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.<br>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 | T-Systems Trust Center is maintaining a couple of root certificates and appropriate SubCAs, issuing all of the following types of EE certificates (but not all are provided by each of the SubCAs): SSL server certificates, Secure mail protocols (SMTPS), S/MIME email certificates, Code signing certificates.<br>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.<br>Therefore relying parties can be the public consumer market as well as internal enterprise employees. |
| CA Contact Information | CA Email Alias: telesec_support@t-systems.com<br>CA Phone Number: +49 1805 268 204<br>Title / Department: Trust Center Services |

**Technical information about each root certificate**

| | |
|---|---|
| Certificate Name | T-TeleSec GlobalRoot Class 3 |
| Certificate Issuer Field | CN = T-TeleSec GlobalRoot Class 3<br>OU = T-Systems Trust Center<br>O = T-Systems Enterprise Services GmbH<br>C = DE |
| Certificate Summary | T-Systems plans to offer certificates with a high security level (e.g. EV) chaining up to this "T-TeleSec GlobalRoot Class 3" root. High security level services for email and code signing will also be created, and the corresponding Sub-CAs will be operated under this Class 3 root. This Class 3 root will only have internally-operated subordinate CAs. T-Systems currently offers certificates with a standard security level (e.g. OV) chaining up to the currently included "Deutsche Telekom Root CA 2" root. All of those standard security services will eventually chain up to a "T-TeleSec GlobalRoot Class 2" root. Inclusion of the "T-TeleSec GlobalRoot Class 2" root is not currently part of this request. |

| | |
|---|---|
| Root Cert URL | http://www.telesec.de/downloads/GlobalRoot_Class_3.cer |
| SHA1 Fingerprint | 55:A6:72:3E:CB:F2:EC:CD:C3:23:74:70:19:9D:2A:BE:11:E3:81:D1 |
| 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 | https://root-class3.test.telesec.de |
| CRL URL | http://pki.telesec.de/rl/GlobalRoot_Class_3.crl<br>http://crl.serverpass.telesec.de/rl/EV_SSL_CA_Class_3.crl (NextUpdate: 24hours)<br>ServerPass CP/CPS section 4.9.7: The certificate revocation list (CRL), which contains the revoked certificates of end entities, is updated twice a day and published by the repository. |
| OCSP URL | OCSP URI in EE Cert: http://ocsp.telesec.de/ocspr<br>OCSP URI in EV Intermediate Cert: http://ocsp.serverpass.telesec.de/ocspr<br><br>Please provide the sections of your CP/CPS specifying availability and update requirements for the OCSP service.<br>CA/Browser Forum's EV Guidelines Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."<br>>> We will draft a new CPS Version for EV Service "ServerPass EV" and include it within chapter 4.9.9 Online availability of revocation/status information<br><br>Please also perform this EV Testing: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version<br>>> Test browser loaded & installed; Root cert included in local root store;<br>We would like to ask for support as offered on Mozilla's web site to create an "ASCII-encoded representation of the DER encoding" of our root certificate. Whom may I contact regarding this task?<br>>> See https://bugzilla.mozilla.org/show_bug.cgi?id=669849#c10 |
| Requested Trust Bits | Websites (SSL/TLS) |
| SSL Validation Types | EV |
| EV Policy OID(s) | 1.3.6.1.4.1.7879.13.24.1 |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | This "T-TeleSec GlobalRoot Class 3" root will have internally-operated subordinate CAs corresponding to the high security services that are offered. |
| Externally Operated SubCAs | None. There will not be externally operated subCAs under this root. |
| 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 3" root cert. |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | Repository: http://www.telesec.de/pki/roots.html<br>CP (English): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cp_en.pdf<br>CP (German): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cp.pdf<br>CPS (English): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cps_en.pdf<br>CPS (German): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cps.pdf<br>ServerPass CP/CPS (German): http://www.telesec.de/serverpass/cps.html<br>ServerPass CP/CPS v1.1 (English): https://bugzilla.mozilla.org/attachment.cgi?id=555341 |
| Audits | Audit Type: WebTrust for CA and EV<br>Auditor: Ernst & Young GmbH<br>Auditor Website: http://www.ey.com/DE/de/Home/Home<br>WebTrust for CA Audit Report: http://cert.webtrust.org/SealFile?seal=1148&file=pdf (2010.12.17)<br>WebTrust EV Audit Report: https://cert.webtrust.org/SealFile?seal=1090&file=pdf (2010.06.20) |
| Organization Verification Procedures | ServerPass CP/CPS section 3.2.2, Identity check on an organization<br>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:<br>Legal person: The request form signed by an authorized signatory.<br>Authority: The request form signed by an authorized representative of the authority and stamped with the official seal.<br>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.<br>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.<br><br>The following is checked for all business categories:<br>• Is the information on the request form identical to the information in the Certificate Signing Request (CSR) of the online request?<br>• 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)?<br>• The authorization of the responsible contact at the organization named in the request (legal person),<br>• 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?<br>• 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<br>• Are any necessary Whois entries available.<br>Additional checks are carried out as required.<br><br>TeleSec ServerPass EV: The initial request can only be placed after successful registration in the customer portal <myServerPass>. The required checks are carried out in accordance with [WTEVGUIDE].<br>[WTEVGUIDE] = Guidelines For The Issuance and Management Of Extended Validation Certificates, The CA / Browser Forum Version 1.2, October 1, 2009 |

| | |
|---|---|
| SSL Verification Procedures | ServerPass section 3.2.2: The following is checked for all business categories: …<br>• 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?<br>• 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<br>• Are any necessary Whois entries available.<br><br>Additionally there is an "Operation Manual" for Trust Center staff including employees working on the registration and validation procedure. To summarize, www.denic.de is the first tool which is used to verify the ownership of a domain under TLD .de , which most of the issued certificates are. For international TLD WHOIS is used instead (www.whois.net). The domainholder must be the same organization stated within the O field of the certificate. If this is not the case, a letter of attorney is needed stating, that the one applying for the certificate is acting on behalf of the domain owner. |
| Email Address Verification Procedures | N/A – Not requesting the email trust bit at this time. |
| Code Signing Subscriber Verification Procedures | N/A – Not requesting the code signing trust bit at this time. |

**Response to Mozilla's 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 | This Class 3 root will only have internally-operated subordinate CAs. |
| Audit Criteria | WebTrust CA and EV audits are performed annually. |
| Document Handling of IDNs in CP/CPS | N/A |
| Revocation of Compromised Certificates | 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).<br>All certificates will have to include the URI for the OCSP responder:<br>CA: http://ocsp.telesec.de/ocspr<br>EE: http://ocsp.serverpass.telesec.de/ocspr |

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

| | |
|---|---|
| Long-lived DV certificates | N/A – SSL certs issued under his root are EV |
| Wildcard DV SSL certificates | N/A – SSL certs issued under his root are EV |
| Email Address Prefixes for DV Certs | N/A – SSL certs issued under his root are EV |
| Delegation of Domain / Email validation to | There will be no externally-operated Sub-CAs or RAs for the certificates in the hierarchy of this Class |

| | |
|---|---|
| third parties | 3 root. Only internal RAs may verify certificates issued in the hierarchy of this Class 3 root. |
| Issuing end entity certificates directly from roots | N/A, root CA will NEVER issue EE certificates |
| Allowing external entities to operate subordinate CAs | Externally-operated subCAs are not allowed under the Class 3 root. |
| 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 | Validation procedures for .int domains are the same as for all other TLD.<br>T-Systems Trust Center has followed the recommended "internal" audit and there were no issues found. RA employees are aware of the issues. The topic is discussed during the regular scheduled trainings.<br>The Operation Manual describes the various types of TLD (generic, sponsored, unsponsored, country-code, infrastructure). It is stated, that .int is a sponsored (IANA) TLD for multi-national organizations, which has to be validated by the internal RA. |
| 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 includes contact details for any question or comment. This is not limited to entities or people having any kind of contract with T-Systems. |