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. 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. 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.
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 3
Certificate Issuer Field	CN = T-TeleSec GlobalRoot Class 3 OU = T-Systems Trust Center O = T-Systems Enterprise Services GmbH C = DE
Certificate Summary	Root certificate "T-TeleSec GlobalRoot Class 3" is intended to replace the already included root certificate "Deutsche Telekom Root CA 2" in a long term run. Only solutions (SubCAs) issuing EV certificates will be allowed to be maintained under this root. All non-EV certificates will be run under a different root. -- How about the email and code signing certs that you plan to issue in the future? How about the externally-operated sub-CAs currently chaining up to the "Deutsche Telekom Root CA 2" root certificate?

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 http://crl.serverpass.telesec.de/rl/EV_SSL_CA_Class_3.crl (NextUpdate: 24hours) Please provide the sections of your CP/CPS documentation that state the requirements about frequency of updating CRL. Note the CA/Browser Forum's EV guidelines: CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days
OCSP URL	OCSP URI in EE Cert: http://ocsp.telesec.de/ocspr OCSP URI in EV Intermediate Cert: http://ocsp.serverpass.telesec.de/ocspr Please provide the sections of your CP/CPS specifying availability and update requirements for the OCSP service. 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." Please also perform this EV Testing: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	Websites (SSL/TLS) Comment from T-Systems: We plan to introduce products for Email (S/MIME) and Code Signing in the future / we would like to discuss what the best approach will be in order to ensure that appropriate trust bits are embedded within Mozilla products before starting issuing certificates If you would like to also request that the email and code signing trust bits be turned on, then you will need to provide (in publicly available and audited documentation) the information listed in #4 and #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices And the documented practices must meet the requirements of the Mozilla CA Certificate Policy.
SSL Validation Type	OV, EV
EV Policy OID(s)	1.3.6.1.4.1.7879.13.24.1

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 "T-TeleSec-GlobalRoot-CP". This Root CA will replace the already included "Deutsche Telekom Root CA 2". At the moment all certificates are still issued under this old root certificate. Once we have embedded the new "T-TeleSec GlobalRoot Class 3" into the most important products, we will start issuing certificates using the new root anchor and appropriate Sub CAs. As of now, there is only one Sub CA operating, which has issued the needed test certificate for the embedding process.
Externally Operated SubCAs	Currently None https://bugzilla.mozilla.org/show_bug.cgi?id=378882#c130 "* The Deutsche Telekom Root CA 2 certificate currently has 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 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 two sub-CAs that chain up to the Deutsche Telekom Root CA 2 certificate, one issues end-entity certificates for employees, the other for machines." … "* The FhG (externally-operated sub-CA) has two internally-operated subordinate CAs. One sub-CA provides certification services to their own employees, and the other sub-CA issues certificates for their own machines. All FhG employees are registered within their own SIGMA system. They also maintain a central list of registered services/machines. " Does the "Deutsche Telekom Root CA 2" root cert have any additional externally-operated sub-CAs? Will these externally operated subCAs be migrated to this new root? The CPS seems to allow for externally-operated subCAs under this new root. If this is the case, then the information in the subCA checklist will also need to be provided: https://wiki.mozilla.org/CA:SubordinateCA_checklist
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 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 (English): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cps_en.pdf CPS (German): http://www.telesec.de/pki/service/GlobalRoot_Class_3/cps.pdf 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://agb.telekom.de/doku/datei/38713.pdf
Audits	Audit Type: WebTrust for CA and EV Auditor: Ernst & Young GmbH Auditor Website: http://www.ey.com/DE/de/Home/Home WebTrust for CA Audit Report: http://cert.webtrust.org/SealFile?seal=1148&file=pdf (2010.12.17) WebTrust EV Audit Report: https://cert.webtrust.org/SealFile?seal=1090&file=pdf (2010.06.20)
Organization Verification Procedures	Where is the CP/CPS documentation regarding organizational verification procedures for EV SSL certs? CPS: 3.2.2 Authentication of an organization The basic requirement for commissioning a certification authority is the conclusion of a contract. This contractual relationship is generated by T-Systems sales units with legal help. The following validation procedures apply in relation to the authentication of organizations: - Ascertaining that the organization exists - Verifying the company name and the business address To carry out the validation process, the CA or the RA use the organization documents issued by a public body or authority. The authentication of organizations is subject to requirements that correspond to the security level. Please refer to Section 3.2.4. 3.2.3 Authentication of a natural person The authentication of natural persons is subject to the following requirements. 3.2.3.1 High security level The following validation procedures must be carried out to identify a natural person who requests services with a high security level □ Ascertaining that the natural person exists based on identification features that can be verified. □ Personal appointment at a CA or RA with an officially issued passport document with photo. In order to verify such identification features, the CA or RA can access an identity verification service recognized by T-Systems or an identity verification database of a third party or the organization documents issued by a public body or authority. 3.2.4 Unverified information The information required for the authentication is checked, see Section 3.2. Other information will not be checked. **Sections 3.2.2 and 3.2.4 in the CPS refer to each other. Where exactly is the information about authentication of organizations according to security level that section 3.2.2 refers to?**

	CP: 3.2.2 Authentication of an organization Organizations are authenticated in accordance with the requirements laid down in the relevant CPS. 3.2.3 Authentication of a natural person Natural persons are authenticated in accordance with the requirements laid down in the relevant CPS. 3.2.3.1 Medium security level The following validation procedures must be carried out to identify a natural person who requests services with a medium security level □□ Ascertaining that the natural person exists based on identification features that can be verified. In order to verify such identification features, the CA or RA can access an identity verification service recognized by T-Systems or an identity verification database or the passport documents issued by a public body or authority. Natural persons are authenticated in accordance with the requirements laid down in the relevant CPS. Every certification authority will perform reliable checks in a suitable manner. 3.2.3.2 High security level The following validation procedures must be carried out to identify a natural person who requests services with a high security level □ The requirements for the medium security level must be met. □ Personal appointment at a CA or RA with an officially issued passport document with photo Natural persons are authenticated in accordance with the requirements laid down in the relevant CPS. Every certification authority will perform reliable checks in a suitable manner. 3.2.4 Unverified end subscriber information Unverified end subscriber information is information that is included in the certificate without being checked. Please see the relevant CPS for details. **Please see section 7 of http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html** **"all information that is supplied by the certificate subscriber must be verified by using an independent source of information or an alternative communication channel before it is included in the certificate;"** 3.2.5 Authorization to sign The authorization of a natural person as being entitled to act on behalf of an organization or a natural person must take place in accordance with an adequate procedure that is described in the CPS. This particularly applies in the case of function/group/machine or server certificates or where certification orders are placed by a registration authority. **What section of the CPS is that referring to?**
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 "Organisation" (O) field. This may not be the organisation 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 organisation for this subject matter. Please provide the URL(s) and section number(s) where this information may be found in your CP/CPS documents. Mozilla CA Certificate Policy: http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html "6. We require that all CAs whose certificates are distributed with our software products: + provide some service relevant to typical users of our software products; + publicly disclose information about their policies and business practices (e.g., in a Certificate Policy and Certification Practice Statement);" and "7. We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: + all information that is supplied by the certificate subscriber must be verified by using an independent source of information or an alternative communication channel before it is included in the certificate; + for a certificate to be used for digitally signing or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate or has been authorized by the email account holder to act on the account holder's behalf; + for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate or has been authorized by the domain registrant to act on the registrant's behalf; + for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate or has been authorized by the entity referenced in the certificate to act on that entity's behalf;"
EV SSL Verification Procedures	Where are the domain control validation procedures described for the EV SSL certs?
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	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 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). 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)

Long-lived DV certificates	N/A – SSL certs are OV and EV
Wildcard DV SSL certificates	N/A – SSL certs are OV and EV
Email Address Prefixes for DV Certs	N/A – SSL certs are OV and EV
Delegation of Domain / Email validation to third parties	N/A, validation procedure is not delegated See above. Also, the CP has provision for RAs.
Issuing end entity certificates directly from roots	N/A, root CA will NEVER issue EE certificates
Allowing external entities to operate subordinate CAs	N/A, there are only internal Sub CAs for "T-TeleSec GlobalRoot Class 3" See above.
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. – Where is this documented? 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.
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.