Bugzilla ID: 436467
Bugzilla Summary: Add new TC Universal III Root certificate

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.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	TC TrustCenter GmbH
Website URL	http://www.trustcenter.de
Organizational type	Commercial CA and has several accreditations, incl. German Signature Act, SISAC, ETSI.
Primary market / customer base	Based in Germany and have customers in all major regions of the world. TC TrustCenter offers a variety of products and services including SSL Server certificates and Email certificates.
CA Contact Information	CA Email Alias: root-distribution@trustcenter.de CA Phone Number: 49-40-8080260 Title / Department: Director Product Management

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	TC TrustCenter Universal CA III
Description	This root will have an internally-operated subordinate CA for each registration strength; "Class 1", "Class 2", "Class 3" and "Class 4 EV". This root currently has one Class 4 EV subordinate CA, "TC TrustCenter Class 4 Extended Validation CA I", which will only issue EV certificates. This new root will co-exist with the "TC TrustCenter Universal CA I" root that is currently included in NSS. This new root will effectively replace the "TC Universal CA II" root which was not included in NSS. For this new root, TC TrustCenter generated a new key (supervised by their auditor) to be compliant with the CA/B Forum guidelines.
URL of root cert	https://bugzilla.mozilla.org/attachment.cgi?id=411063
SHA-1 fingerprint.	96:56:cd:7b:57:96:98:95:d0:e1:41:46:68:06:fb:b8:c6:11:06:87
Valid from	2009-09-09
Valid to	2029-12-31
Cert Version	3
Modulus length	2048
Test Website(s)	Valid certificate: https://testserver.universal-iii.trustcenter.de Revoked certificate: https://testserver-revoked.universal-iii.trustcenter.de Expired certificate: https://testserver-expired.universal-iii.trustcenter.de

CRL	http://crl.tcuniversal-III.trustcenter.de/crl/v2/tc_universal_root_III.crl (NextUpdate 7 days) http://crl.I.tcclass4.tcuniversal-III.trustcenter.de/crl/v2/tc_class4_EV_CA_I.crl (NextUpdate 7 days) Other TC TrustCenter URLS: http://www.trustcenter.de/crl CPS section 4.9.7: In general, CRLs are issued at least once a day, but they may be updated several times a day, even if no changes have occurred since the last issuance. Each CRL has a maximum validity period of one week. CRLs for CAs issuing very few certificates (e.g. Root CAs) may have a longer validity.
OCSP	http://ocsp.tcuniversal-iii.trustcenter.de http://ocsp.I.tcclass4.tcuniversal-III.trustcenter.de CPS Section 4.9.9: If a CA provides revocation information via OCSP, that service is updated at least once every day. OCSP responses have a maximum expiration time identical to the validity of the associated CRL. (7 days)
CA Hierarchy	This root currently has one sub-CA with CN “TC TrustCenter Class 4 Extended Validation CA I”, which will only issue EV certificates. http://www.trustcenter.de/media/pr_TC_Class_4_EV_CA_I.der There are currently no concrete plans for other sub-CAs. In the future, TC TrustCenter may issue a "TC Class 3 L1 CA xx", "TC Class 2 L1 CA yy" or ""TC Class 1 L1 CA zz" from this "TC Universal CA III". The "TC Universal CA III" will not have a "TC Class 0" Sub-CA.
Sub-CAs operated by 3rd parties	Currently None. While not currently in plan, it is possible that this root will eventually have externally operated sub-CAs. If that does happen, TC TrustCenter plans to follow the Mozilla policy, and such externally operated sub-CAs would be limited to certificate policy OID different from the EV certificate policy. The company operating it would either use it for internal purposes or have an appropriate ETSI or WebTrust audit. TC TrustCenter does not plan to have externally operated EV-Sub-CAs.
Cross-signing	None currently, none planned
Requested Trust Bits	Websites Email Code Signing
If SSL: DV, OV, and/or EV	OV, EV CPS section 3.2: “Certificates not containing the name of an individual person (e.g. SSL certificates containing the full qualified domain name of a web server or Team-certificates identifying a group of persons) are always assigned to an organization.” CPS section 3.2.2: “A corporate organizational entity must provide a proof of its existence. This verification may be carried out by the presentation of a document, which proves the existence of the organization”
EV policy OID(s)	1.2.276.0.44.1.1.1.4.
CP/CPS	CPS (English): http://www.trustcenter.de/media/CPS-TCTrustCenter-en.pdf CPD (English): http://www.trustcenter.de/media/CPD-TCTrustCenter-en.pdf CPD for EV (German): http://www.trustcenter.de/media/CPD_TCTrustCenter_EV-de.pdf CPD for EV (English): https://bugzilla.mozilla.org/attachment.cgi?id=455642 TC TrustCenter’s CPD defines the authentication of individual entities in more detail. All root certs: http://www.trustcenter.de/infocenter/root_certificates.htm

AUDIT	Audit Type: ETSI EV audit (ETSI TS 102042 v2.1.1) Auditor: TÜV-IT Germany Auditor WebSite: http://www.tuvit.de/ ETSI EV Certificate: http://www.tuvit.de/certuvit/pdf/6711UE_s.pdf (2009.11.06) http://www.tuvit.de/english/47347.asp Both the root, “TC TrustCenter Universal CA III”, and the EV sub-CA “TC TrustCenter Class 4 Extended Validation CA I” are noted in the ETSI EV certificate.
Registration Authorities	CPS section 1.3.2: A Registration Authority (RA) works on behalf of a CA. TC TrustCenter operates an in-house Registration Authority but may also make use of external service providers as subsidiary RAs responsible for verifying both business information and personal data contained in a subscriber’s certificate. *Any subsidiary RA is contractually bound to TC TrustCenter. A subsidiary RA is registered as registration service provider. The Registration Officers of such a subsidiary RA are individually identified; they are equipped with special Registration Officer (RO) certificates. Only data signed by an RA is accepted by the CA system. *TC TrustCenter reserves the right to prohibit performing RA services on behalf of TC TrustCenter, if an RA does not conform to the provisions set forth in this CPS.
Identity Verification	CPS section 3.2.4: Class 0 certificates are issued for testing and demonstration purposes. They are valid for a short period of time only. Data contained in a Class 0 certificate is not verified by TC TrustCenter in any way! CPS section 3.2.4: Class 1 certificates always contain an e-mail address. They confirm that the e-mail address stated in the certificate existed at the time of application and that the owner of the public key had access to this e-mail address. Class 1 certificates provide very little evidence of the identity of the certificate holder. Except from the existence and the accessibility of the e-mail address, none of the data contained in the certificate has been verified. CPS section 3.2.4: Information that is not verified will not be included in TC Class 2, TC Class 3, and TC Class 4 certificates. CPD section 4.3: Statements made in a Class 2 certificate regarding natural persons, if such are included, are verified in the following way: …Statements about a natural person’s name are verified by a) confirmation of an accredited third party regarding the correctness and the completeness or by b) confirmation of the information by presentation of a copy of an official photo ID document with signature. CPD section 4.4: Class 3 certs If a natural person is named in a Class 3 certificate, the personal appearance and the presentation of a valid official photo ID is necessary. The verification of the identity of the certificate holder may either take place in a branch office of the German Post utilizing the Post Ident® procedure, in a TC TrustCenter IdentPoint® (an authorized IdentPoint® of the organization), or with another representative of TC TrustCenter, authorized to perform the identity verification. A notary public is also eligible. CPD section 4.4.2 describes the verification of statements regarding organizations

	CPD for EV section 3: All EV Certificates issued by TC TrustCenter are compliant to this document (TC TrustCenter Certificate Policy Definitions for EV Certificates) and the “Guidelines for the Issuance and Management of Extended Validation Certificates.” CPD for EV section 3.6, Verification of Organizations: Before issuing an EV Certificate, TC TrustCenter must ensure that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, this EV-CPD and matches the information confirmed and documented by TC TrustCenter pursuant to its verification processes. Such verification processes accomplish the following: (1) Verify Applicant’s existence and identity, including; (a) Verify Applicant’s legal existence and identity (as more fully set forth in Section 3.6.1 below), (b) Verify Applicant’s physical existence (business presence at a physical address), and (c) Verify Applicant’s operational existence (business activity). (2) Verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate; (3) Verify Applicant’s authorization for the EV Certificate, including; (a) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester; (b) Verify that Contract Signer signed the Subscriber Agreement; and (c) Verify that a Certificate Approver has signed or otherwise approved the EV Cer-tificate Request
Domain Name Ownership / Control – Non-EV	CPD section 4.3.2: For SSL or device certificates it is checked whether the domain name in the certificate is registered to the organization applying for the certificate, if the domain is registrable. If a domain can not be registered with an official domain registrar an authorized person must confirm that a device with the name in question exists in the internal network, and that a certificate for this device shall be issued. Because the assignment of names to devices must be unique, TC TrustCenter reserves the right to reject applications with internal domain names which have previously been assigned to another organization. Certificates intended for an organization’s internal use containing a non-registrable domain name, e.g. domain.local or domain.internal, must provide additional information in the domain name to allow for a unique assignment to exactly one organization. CPD section 4.4.2: For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate.
Domain Name Ownership / Control – EV	CPD for EV section 3.7 provides the details about how TC TrustCenter verifies that the Applicant is a registered holder of the domain name to be included in the EV Certificate, or has exclusive control of the domain name. The steps include contacting the registered domain holder using the information obtained from WHOIS or through the domain registrar.
Email Address Ownership / Control	TC TrustCenter’s CPS and CPD state that if an e-mail address is contained in the certificate, its correctness is verified by an access test.

	CPS section 3.2.3: Class 1: These certificates always contain an e-mail address. They confirm that the e-mail address stated in the certificate existed at the time of application and that the owner of the public key had access to this e-mail address. … Except from the existence and the accessibility of the e-mail address, no data contained in the certificate is being checked. Class 2: E-mail addresses are verified in the same way as for class 1 certificates. Class 3: E-mail addresses are verified in the same way as for class 1 certificates. CPD section 4.2: Class 1 certificates always contain an e-mail address. Class 1 certificates confirm that the email address stated in the certificate existed at the time of application and that the owner of the public key had access to this e-mail address. Class 1 certificates provide very little evidence of the identity of the certificate holder. Except from the existence and the accessibility of the e-mail address, no data contained in the certificate is being checked. CPD section 4.3.1: Statements made in a Class 2 certificate regarding natural persons, if such are included, are verified in the following way: if the certificate contains an e-mail address, its correctness is verified by an access test. Alternatively, for members of organizations a responsible person in that organization may confirm the correctness of the e-mail address. CPD section 4.4.1 Class 3 Certs: verification of statements about a natural person covers the following points: If an e-mail address is contained in the certificate, its correctness is verified by an access test. If statements about an organization are made in the certificate, the organization itself may confirm the correctness of the e-mail address.
Identity of Code Signing Subscriber	TC TrustCenter's CPS and CPD describe reasonable measures to verify the identity and authorization of the certificate requester. (See sections 3.2 and 4.3 of the CPS.) CPD section 5.2: OU (Organizational Unit): This field may be used for specifying the department within the organization that the certificate is attributed to. In code signing certificates TC TrustCenter will automatically enter the name of the software used for generating the signature. CPD for EV section 2.1 describes information about EV Code Signing Certificates, such as validity period, private key protection, and cert content.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates ○ SSL certs are OV. • Wildcard DV SSL certificates ○ SSL certs are OV. • Delegation of Domain / Email validation to third parties ○ **Applies**. Comment #9: TC TrustCenter's external RAs are contractually bound to adhere to the procedures specified in TC TrustCenter's CPS and other relevant policies. RAs are not allowed to use their own procedures and deviate from TC TrustCenter's policies. How we verify that external RAs are adhering to our CPS:

	▪ We distinguish between Local Registration Officers and External Registration Officers. ▪ The Local Registration Officers are limited regarding their tasks. They cannot vet organizations and domains. They can only perform personal vetting for a limited and previously named set of organizations. Local Registration Officers have been empowered by all affected organizations to perform that role. ▪ External Registration Officers are allowed to vet organizations and Domains. They have to undergo a special training on the procedures. ▪ Both, Local Registration Officers and External Registration Officers are contractually bound to adhere to our CP/CPS. We perform random checks and we perform checks in case of abnormalities • Issuing end entity certificates directly from roots o No. Root only signs sub-CAs. • Allowing external entities to operate unconstrained subordinate CAs o No plans to have external entities operate sub-CAs from this root. • Distributing generated private keys in PKCS#12 files o **Applies**. Comment #9: PKCS#12 files are encrypted in our system. User can choose to receive the password for the PKCS#12 PSE as an SMS (instead of an email). The PKCS#12 file is not attached to the email but must be downloaded from a URL with password protection. This approach is particularly convenient for customers asking for key recovery (e.g. for email encryption certificates). • Certificates referencing hostnames or private IP addresses o All EV certificates must have a name resolvable using DNS. In general, Private IP addresses and unqualified host names (e.g. myserver) are not allowed. • OCSP Responses signed by a certificate under a different root o No. Test website cert has AIA extension specifying OCSP, and the website loads into Firefox without error when OCSP is enforced. • CRL with critical CIDP Extension o No. CRLs import into Firefox without error. • Generic names for CAs o Name is not generic.