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**: certificate@trustcenter.de An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. **CA Phone Number**: 49 (0)40 808026-0 A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. **Title / Department**: Certification Practice Administrator If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

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	What is the relation between this root and "TC TrustCenter Universal CA I", which is already included in NSS? What is the relation between this root and "TC TrustCenter Universal CA II", which has been postponed? This root will have an internally-operated subordinate CA for each registration strength; "Class 1", "Class 2", "Class 3" and "Class 4". This root currently has one Class 4 subordinate CA, "TC TrustCenter Class 4 Extended Validation CA I", which will only issue EV certificates. Will this root have a Class 0 sub-CA?
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	https://testserver.universal-iii.trustcenter.de/ -- My Firefox browser can't find this server.
CRL	http://crl.tcuniversal-III.trustcenter.de/crl/v2/tc_universal_root_III.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 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 Please list the other current and planned sub-CAs for this root, and what their purpose will be.
Sub-CAs operated by 3rd parties	Currently None Can this root have externally-operated sub-CAs in the future? What about the EV sub-CA? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b.
Cross-signing	None currently, none planned
Requested Trust Bits	Websites Email Code Signing
If SSL: DV, OV, and/or EV	DV, OV, EV Comment #5: The "TC Universal CA III" root certificates will be used to issue DV, OV and EV certificates (using different Sub-CAs). It seems to me that SSL certs are not ever DV… 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" So, can SSL certs be issued from Class 0 or Class 1?
EV policy OID(s)	1.2.276.0.44.1.1.1.4.
CP/CPS	CPS as approved by the ETSI EV audit (English): https://bugzilla.mozilla.org/attachment.cgi?id=411145

	CPS URL: http://www.trustcenter.de/cps Certificate Policy URL (CPD): http://www.trustcenter.de/cpd CPD in English: http://www.trustcenter.de/media/CPD-TCTrustCenter-061023-en.pdf 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.
Organization Identity Verification	CPS section 3.2 Initial identity validation In order to obtain a certificate, any applicant must apply for a certificate, and identify and authenticate themselves to TC TrustCenter. TrustCenter groups the certificates into “certificate classes“. The higher the certificate class, the more extensive are the identification verifications that are being used as a basis for the issuance of the certificate. The certificates themselves contain information regarding the class of the certificate for anyone who wishes to rely on the certificate. Within the context of classification into certificate classes a distinction is made between individuals and organizations. Certificates for individuals who do not provide information about their affiliation to an organization do not contain statements about the subject’s organizational affiliation. Organizational certificates always contain a statement regarding an organization. These certificates may either be attributed to an organization (such as device certificates which cannot be attributed to natural persons) or they may be attributed to a member of an organization, such as an employee of a company. Information about an organization must be entered into all organizational certificates. 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. This section covers these topics in a general fashion. Please see the Certificate Policy Definitions (CPDs) for further details. 3.2.2 Authentication of organization identity 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 (current extract of a competent official register in which the organization is listed or a comparable document). For Class 2 certificates copies of such documents are sufficient, Class 3 and above require the presentation of original documents or notarized copies. Further details, especially additional requirements on the validity of such documents can be found in TC TrustCenter’s CPDs for the certificate class under consideration. Alternatively, data provided by reputable third party vendors of business information will be accepted as well. Governmental or administrative authorities must supply documents which reflect their relationship to the next higher entity

(e.g. a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer. Other organizational entities must provide proper proof of existence/registration that is comparable to the above.

3.2.3 Authentication of individual identity

The authentication of an individual entity depends on the certificate class.

Class 0: These 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!

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. 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.

Class 2: These certificates contain data about the certificate owner. E-mail addresses are verified in the same way as for class 1 certificates. To verify the correctness of additional data contained in a class 2 certificate (e.g. name and affiliation) the applicant must present copies of documents proving the correctness of this data.

Class 3: These certificates may contain the same data as class 2 certificates. E-mail addresses are verified in the same way as for class 1 certificates. To verify the correctness of additional data contained in a class 3 certificate (e.g. name and affiliation) the applicant must present original documents proving the correctness of this data. Original documents may be replaced by notarized copies.

Class 4: These certificates are issued based on the requirements of Extended Validation Certificates: Guidelines for the Issuance and Management of Extended Validation certificates, Version 1.1, CA/Browser Forum, http://www.cabforum.org.

TC TrustCenter will not issue EV Certificates before having undergone and passed an annual

(i) WebTrust Program for CAs audit and

(ii) WebTrust EV Program audit, or

(iii) an equivalent audit for both (i) and (ii) as approved by the CA/Browser Forum.

TC TrustCenter's CPDs define the authentication of individual entities in more detail. The CPDs can be found at http://www.trustcenter.de/cpd.

3.2.4 Non-verified subscriber information

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!

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.

Information that is not verified will not be included in TC Class 2, TC Class 3, and TC Class 4 certificates.

Information about subscriber's internal details (e.g. name of Organizational Unit (OU in the Distinguished Name of the certificate) must be provided by the applicant and has to be approved by the organization. Verification of the OU through a

	third party is not performed. 3.2.5 Validation of authority TC Class 2, TC Class 3, and TC Class 4 certificates that contain explicit or implicit information about the applicant’s affiliation are issued only after ascertaining that the applicant has the authorization to act on behalf of the organization in the asserted capacity. 4.3.1 CA actions during certificate issuance TC TrustCenter verifies, as set forth in section 3.2.1, that the applicant is in possession of the private key and that the certificate request has the proper contents, for example a server certificate request must state the fully qualified server and domain name in the “Common Name” field. TC TrustCenter verifies the data contained in the request according to this CPS and according to the applicable CPD.
Domain Name Ownership / Control	CPD section 4.3.2: For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate. In contrast to that, an automatic verification of the existence on an organizational unit (which can be stated in the OU field of the certificate) is usually not possible. A domain registration may be checked in advance. When the certificate is issued the domain check must not be more than twelve months old.
Email Address Ownership / Control	TC TrustCenter’s CPS and CPD state that 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. 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. 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. 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: If the CN-field contains "CodeSigning for <content of the O-field> the certificate is a CodeSigning certificate. In this case the data from the O-field (Organization) is automatically copied into the CN-field, because usually the CN-field is displayed when a user verifies program code.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. . For the ones that are applicable, please provide further information. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o Name is not generic.