Bugzilla ID: 392024
Bugzilla Summary: add new TC TrustCenter root certificates

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.

General Information	Data
CA Name	TC TrustCenter GmbH
Website URL (English version)	Website: http://www.trustcenter.de
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	commercial global
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	TC TrustCenter GmbH is a commercial company based in Germany, with customers in all major regions of the world. TC TrustCenter offers a variety of products and services including SSL Server certificates and Email certificates.

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

Note: Another root was included in the original request, TC TrustCenter Universal II. However, this root is not yet operational and has not been covered by an audit. My recommendation is to create a separate bugzilla request for inclusion of the Universal II root. It will not be covered below.

Info Needed	Data	Data	Data	Data
Root CN	TC TrustCenter Class 1 CA	TC TrustCenter Class 2 CA II	TC TrustCenter Class 3 CA II	TC TrustCenter Universal CA I
The root CA certificate URL	http://www.trustcenter.de/certservices/cacerts/tcclass1-2011.der	http://www.trustcenter.de/media/class_2_ii.der	http://www.trustcenter.de/media/class_3_ii.der	http://www.trustcenter.de/media/Universal_CA-I.der
Description	This root has four internally-operated subordinate CAs which issue certificates for email and SSL client authentication. There are many customers who are using certificates chained to this	This root has two internally-operated subordinate CAs which issue certificates for SSL, email, and code signing.	This root has one internally-operated subordinate CA which issues certificates for SSL, email, and code signing.	This root has been introduced to reduce the number of root certificates in the trusted root stores. This root will have internally-operated subordinate CAs for each registration

	root for secure email with Thunderbird.			strength. “Class 1”, “Class 2”, “Class 3” and “Class 4” represent the registration strength. This root currently has one Class 3 subordinate CA. Over time this root will have more “TC Class x” subordinate CA certificates.
SHA-1 fingerprint.	72:0f:c1:5d:dc:27:d4:56:d0:98:fa:bf:3c:dd:78:d3:1e:f5:a8:da	ae:50:83:ed:7c:f4:5c:bc:8f:61:c6:21:fe:68:5d:79:42:21:15:6e	80:25:ef:f4:6e:70:c8:d4:72:24:65:84:fe:40:3b:8a:8d:6a:db:f5	6b:2f:34:ad:89:58:be:62:fd:b0:6b:5c:ce:bb:9d:d9:4f:4e:39:f3
Valid from	09.03.1998	12.01.2006	12.01.2006	22.03.2006
Valid to	01.01.2011	31.12.2025	31.12.2025	31.12.2025
Cert Version	X.509 version 3	X.509 version 3	X.509 version 3	X.509 version 3
Modulus length / key length	RSA 1024 Bit	RSA 2048 bit	RSA 2048 bit	RSA 2048 bit
Comment	“One of your roots is only 1024 bit. NIST recommend that all such roots by phased out by the end of 2010, yet this root expires at the end of 2011. What is your current end-of-life plan with regard to this root?” “The TC TrustCenter Class 1 CA expiring beginning of 2011 will be effectively replaced by TC Universal I. TC TrustCenter Class 2 II and TC TrustCenter Class 3 II will replace the TC TrustCenter Class 2 and TC TrustCenter Class 3 roots. We'll phase out the 1024 bit roots before end of 2010.”			
CRL URL	http://www.trustcenter.de/crl/v2/tcclass1.crl	http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	http://www.trustcenter.de/crl/v2/tc_universal_root_I.crl
CRL Frequency	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.			
OCSP Responder URL	http://ocsp.tcclass1.trustcenter.de/	http://ocsp.tcclass2-ii.trustcenter.de	http://ocsp.tcclass3-ii.trustcenter.de	http://ocsp.tcuniversal-i.trustcenter.de
OCSP responder update frequency	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.			
CA Hierarchy	Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=362215 The subordinate CAs can be downloaded from http://www.trustcenter.de/en/infocenter/root_certificates.htm			
List of CAs	TC TrustCenter Class 1 CA	TC TrustCenter Class 2 CA II	TC TrustCenter Class 3 CA II	TC TrustCenter Universal I

with certificates signed by this root.	has the following sub-CAs: TC Class 1 L1 CA III TC Class 1 L1 CA V TC Class 1 L1 CA VI TC Class 1 L1 CA VII EE Certificate types 1. Email certificates 2. SSL client certificates Not for SSL server certificates	Has the following sub-CAs: TC Class 2-II L1 CA IV TC Class 2-II L1 CA VIII EE Certificate types 1. SSL Server certificates 2. Email certificates 3. SSL client certificates 4. Code Signing certs. 5. IPsec certificates 6. special purpose certs	Has the following sub-CAs: TC Class 3-II L1 CA IV EE Certificate types 1. SSL Server certificates 2. Email certificates 3. SSL client certificates 4. Code Signing certs. 5. IPsec certificates 6. special purpose certs	Has the following sub-CAs: TC Class 3-II L1 CA IX EE Certificate types 1. SSL Server certificates 2. Email certificates 3. SSL client certificates 4. Code Signing certs. 5. IPsec certificates 6. special purpose certs
List subordinate CAs operated by third parties	Currently None The CA's could have sub-CA's in the future. Some of them could actually have ownership/control of the sub_CA key pair and CA. If TC TrustCenter issues a Sub-CA certificate to a third party then there will be contractual agreements in place requiring the third party to adhere to the requirements of the applicable CPS. The entry "Path length" in the "Basic contstraints" extension (marked as critical) is set to 0. So they cannot use their own subordinates.			
cross-signing	None	None	None	None
Requested Trust Bits One or more of: - Websites (SSL/TLS) - Email (S/MIME) - Code Signing	Email	Websites Email Code	Websites Email Code	Websites Email Code
If SSL Specify one of - DV - OV	N/A This root is not to be enabled for SSL.	OV 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.		

- EV		CPS section 3.2.2: Authentication of organization CPS Section 3.2.5: 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. From TC TrustCenter: TC TrustCenter not only verifies that the domain name in the CN attribute is registered to the organization named in the O field of the certificate. TC TrustCenter always performs additional vetting, e.g. verification of the domain holder's registration with official (governmental) authorities and verifying the identity and authorization of the requesting person to apply for a certificate on behalf of the organization under consideration (see CPD).		
EV policy OID	Not EV	Not EV	Not EV	Not EV
Example certificate(s) For SSL: URLs of one or more web servers using the certificate(s).		https://testserver.class2-ii.trustcenter.de/	https://testserver.class3-ii.trustcenter.de/	https://testserver.universal-i.trustcenter.de/
CP/CPS	TC TrustCenter GmbH Certification Practice Statement (CPS) http://www.trustcenter.de/media/CPS-TCTrustCenter-080904-en.pdf TC TrustCenter Certificate Policy Definitions (CPD) http://www.trustcenter.de/media/CPD-TCTrustCenter-061023-en.pdf Installation/Download of TC TrustCenter CA Certificates http://www.trustcenter.de/en/infocenter/root_certificates.htm Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=362215			
Audit	Audit Type: ETSI 102 042 Auditor: TÜV Informationstechnik GmbH			

	Auditor Website: http://www.tuvit.de ETSI Certificate: http://www.tuvit.de/certuvit/pdf/6707UE_s.pdf
Audit Comment	From TC TrustCenter: The roots submitted for inclusion have been audited. The serial numbers of the CAs listed in the new ETSI certificate are referring to the L1 Sub-CA certificates audited by TÜV-IT. Given the fact that we do not issue end entity certificate off the root (but off Sub-CA only) and it doesn't make much sense to audit the Sub-CA issuance by a root TÜV-IT decided to audit the end entity certificate issuance off a representative and active Sub-CAs chained to the roots covered by this audit. The covered roots are identified by their CN (see second line: "TC TrustCenter Class 2 CA II", "TC TrustCenter Class 3 CA II", "TC TrustCenter Universal CA I"). Additionally the ETSI certificate also references the CPS version (i.e. 1.9.1). The CPS v1.9.1 lists the root certificates covered by that CPS with serial numbers and some more details. Please compare the root certificates submitted for inclusion with these.

Review CPS sections dealing with subscriber verification (COMPLETE)
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - CPD section 4.3.2 Verification of statements about organizations for Class 2 certificates
        - For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate.
        - A domain registration may be checked in advance. When the certificate is issued the domain check must not be more than twelve months old.
    - CPD section 4.4.2 Verification of statements regarding organizations for Class 3 certificates
        - For server certificates it is checked if the domain name in the certificate is registered to the organization applying for the certificate.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - 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: 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.

- 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.
  - Section 4.3, Class2: 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.
  - Section 4.4, Class 3: 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.

- Verify identity info in code signing certs is that of subscriber
  - Yes, per CPS and CPD
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(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
  - CPS Section 1.3.2 and 1.3.5.2
  - 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.
- Issuing end entity certificates directly from roots
  - TC TrustCenter issues end entity certificates to the public from subordinate CAs only.
- Allowing external entities to operate unconstrained subordinate CAs
  - Currently none.
  - CA certificate to an external CA contain the entry "Path length" entry in the "Basic contstraints" extension (marked as critical) set to 0. So they cannot generate their own subordinates.
  - If TC TrustCenter issues a CA certificate to an external CA, this CA must present a CPS and other documentation fulfilling TC TrustCenter's requirements. Furthermore this CA must sign a contractual agreement to adhere to all requirements specified in their CPS. In addition, TC TrustCenter reserves the right to perform audits at this CA's site or to claim a third party audit equivalent to the Root CA's audit.
- Distributing generated private keys in PKCS#12 files
  - In general, subscribers must generate their own key pairs.

    - In cases where this is not possible or not practical, TC TrustCenter prefers to generate subscriber keys on smartcards or other cryptographic tokens. These tokens are then delivered to the subscriber. If the use of cryptographic tokens is not possible, TC TrustCenter may generate subscriber's key pairs.
    - For encryption keys subscribers may enter into a contractual agreement for key escrow or key recovery. TC TrustCenter will then store subscriber's key pair in encrypted form in such a way that decryption is only possible under dual control.
    - TC TrustCenter will not store subscriber's private keys without subscribers consent and not without having informed the subscriber about the possible risks.
    - PKCS#12 files are never transmitted through unsecured channels. In most cases TC TrustCenter informs the subscriber about a download location where the subscriber can download the key pair via encrypted channel (e.g. SSL).
- Certificates referencing hostnames or private IP addresses
    - TC TrustCenter may issue certificates containing domain names or IP addresses not reachable from the public internet. Such certificates always contain the name of the organization (in the O attribute). Even if two organizations use the same internal hostnames and/or internal IP addresses the certificates can easily be distinguished because the O attribute differs.
    - TC TrustCenter verifies that the IP address is either (a) non-routable private (e.g. 192.168.x.y) or (b) is registered to the requestor.
- OCSP Responses signed by a certificate under a different root
    - TC TrustCenter's OCSP responders always sign their responses with an OCSP Signing Certificate that is issued by the CA in question.
- CRL with critical CIDP Extension
    - TC TrustCenter makes full CRLs available for download. TC TrustCenter currently does not use CIDP extensions.

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that the did indeed issue this report.
    - Audit posted on the TUVIT website.
- For EV CA's, verify current WebTrust EV Audit done. (the EV root was moved into a separate request)
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issue noted in the audit statement.