

Root CA Bugzilla ID: 378882

Root CA: T-Systems, Deutsche Telekom Root CA 2

This document summarizes the information gathered and verified for subordinate CAs for companies who use their sub-CA to sign other sub-CAs or certificates for other companies or individuals not affiliated with their company. For instance, this document is necessary when the root issues sub-CAs that are used by Certificate Service Providers (CSP). For more background information, see

- https://wiki.mozilla.org/CA:How_to_apply
- https://wiki.mozilla.org/CA:SubordinateCA_checklist

A root with externally-operated sub-CAs needs to provide the following information in their CPS or contractually with the company operating the sub-CA.

Info Needed	Data
Root Name	Deutsche Telekom Root CA 2
List or Description of all of the Subordinate CA's operated by third parties	The CA has 2 subordinate CAs that are operated by third parties: <ol style="list-style-type: none">1. Deutsches Forschungsnetz, DFN2. Fraunhofer Institute
Requirements (technical and contractual) for subordinate CAs in regards to whether or not subordinate CAs are constrained to issue certificates only within certain domains, and whether or not subordinate CAs can create their own subordinates.	<p>Comment #99:</p> <ol style="list-style-type: none">1. A translation for a Draft of our CP2. A translation of a "service description", which will become a mandatory part of the CP (see Draft of CP). This document describes how we handle external Sub CAs. All those regulations apply to both DFN and Fraunhofer. <p>http://pki.telesec.de/service/documents/T-Systems-Root-CP_en.pdf</p> <p>http://pki.telesec.de/service/documents/service-spec_T-Systems-Root-Signing_en.pdf</p> <p>The CP (the German version) and the service description will come into force, if Mozilla has no further recommendations after the discussion. Otherwise we will stay with the previous version until we have come to an agreement about additional changes or extensions. We do this, since we don't want to change the CP without knowing, whether we have to change some of the new parts after the discussion, which would confuse our customers and users.</p> <p>CP section 1.3.2.1, Registration authorities for subordinated CAs "Registration of subordinated CAs of third parties (that not belong to T-Systems and are completely under control of the T-Systems Trust Center) will be performed solely by authorized employees of the T-Systems Trust Center. Principles for contracts and registration are based on the regulations described in the service description „T-Systems Root Signing“ [TSYSROOTSIGN]. Those regulations are mandatory. The actual registration is then based on contractual regulations."</p>

	<p>Service Description section 3, Customer's Duties to Cooperate</p> <ul style="list-style-type: none"> + Constrains sub-CA certificate usage based on contractual agreement. + T-Systems to review/approve their CP/CPS. + Requires annual audit.
<p>Requirements for sub-CAs to take reasonable measures to verify the following information for end-entity certificates chaining up to the root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.</p> <ul style="list-style-type: none"> a) domain ownership/control b) email address ownership/control c) digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate 	<p>Service Description section 3, Customer's Duties to Cooperate</p> <ul style="list-style-type: none"> + Customer CP/CPS demonstrates that in addition to verifying the identity of individuals and organizations, reasonable measures are taken to verify that the subscriber owns/controls the domain referenced in the certificate and the email account associated with the email address referenced in the certificate.
<p>Whether or not the root CA audit includes the sub-CAs.</p> <p>Audit requirements for subordinate CAs with regard to the frequency of audits and who can/should perform them, as per sections 8, 9, and 10 of the Mozilla CA policy.</p>	<p>T-Systems audit does not include the sub-CAs. However, T-Systems performs annual audits of the Customer's sub-CA.</p> <p>Service Description section 2, Services of T-Systems</p> <ul style="list-style-type: none"> + T-Systems perform yearly audits of the Customer's CA environment to check compliance with the agreed policies (typically, on-site audits take no longer than a day). All compliance check results are communicated to the Customer and are treated in confidence.

For each CSP or sub-CA operated by 3rd party, review the CPS and audit to find the following information. It is best if the CP/CPS and audit statements are translated into English.

Info Needed	Data	Data
Sub-CA Company Name	Deutsches Forschungsnetz, DFN	Fraunhofer Institute Fraunhofer Corporate PKI (FhG)
Sub-CA Corporate URL	http://www.pki.dfn.de	http://www.pki.fraunhofer.de/
CPS Links	http://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP_DRAFT_v22-english.pdf	http://pki.fraunhofer.de/cp/Certificate_Policy_Fraunhofer_Corporate_PKI.pdf

	http://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP_v21-english.pdf http://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CPS_v21-english.pdf	http://pki.fraunhofer.de/cp/Certification Practice Statement Fraunhofer Corporate PKI.pdf
CA hierarchy under the sub-CA.	<p>There are three security levels mentioned in the CP. The Global security level is the only one based on the sub-CA for the T-Systems root.</p> <p>For the Global security level, the public key of the PCA is included in a certificate (“DFN-Verein PCA Global – G01”), which was issued by the “Deutsche Telekom Root CA 2”.</p> <p>All CAs at the Global security level are operated by the DFN-Verein.</p>	<p>This sub-CA provides certification services for FhG employees and machines.</p> <p>Within FhG there are two subordinate CA's, one issues end-entity certs for employees, the other for machines.</p>
Determine if there are SSL certs chaining up to the root that are only DV. Eg the Organization is not verified, only the domain name is verified.	<p>IV/OV</p> <p>Section 3.2.3 of CP: For Global security level, the subscriber must be present and must provide photo ID and passport. Proof of belonging to the organization is checked.</p>	<p>IV/OV</p> <p>Individual identity is validated as per section 3.2.3 of the CP and CPS. According to section 3.2.3 of the CPS, the email and (optionally) domain name for windows smartcard login are provided by FhG after individual identity has been confirmed.</p>
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/ . a) domain ownership/control b) email address ownership/control c) digitally signing code	<p>http://www.pki.dfn.de/fileadmin/PKI/DFN-PKI_CP_DRAFT_v22-english.pdf</p> <p>DFN will move the DRAFT CP into final when public discussion confirms this is sufficient.</p> <p>"3.2.2 Authentication of an organization identity: [...] If a domain name is used in a certificate, the organization's right to use the domain name is verified by DFN-Verein as the PCA."</p> <p>Comment #110: This is what DFN is doing. Before signing a contract</p>	<p>Section 3.2.3 of CPS: the FhG institutes provide the email address and the domain name for the applicant. The SIGMA system contains identity information.</p> <p>Section 3 of the CP: Identification and Authentication.</p> <p>CP Section 1.3.2: Local RAs are responsible for the verification of the identity of employees and the authenticity of machines. The central RA is then responsible for verifying and approving the information provided by the Local RAs.</p> <p>Section 3.2.3 of CP: All FhG employees are registered within the SIGMA</p>

<p>objects -- entity submitting the certificate signing request is the same entity referenced in the certificate</p>	<p>DFN will check, what domains belong to the contractor, and afterwards each certificate issued by the contractor will be checked, whether the certificate belongs to those domains or not.</p> <p>Verification of email address ownership: Section 3.2.3 of CP: the e-mail address must be present and checked during in-person registration.</p>	<p>system. Services/machines are included in a central list of registered services/machines. Subscribers must be personally present with ID cards and passports.</p>
<p>Review the CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.</p>	<p>1.1 Long-lived DV certificates Certs are IV/OV, not DV</p> <p>1.2 Wildcard DV SSL certificates Wildcard certs are not permitted as per CP.</p> <p>1.3 Issuing end entity certificates directly from roots No</p> <p>1.4 Allowing external entities to operate unconstrained subordinate CAs No other subordinate CAs under this sub-CA. All operation of this sub-CA is internal to DFN.</p> <p>1.5 Distributing generated private keys in PKCS#12 files No</p> <p>1.6 Certificates referencing hostnames or private IP addresses Not found.</p> <p>1.7 OCSP Responses signed by a certificate under a different root N/A</p> <p>1.8 CRL with critical CIDP Extension CRLs from http://www.pki.dfn.de/index.php?id=gridcrl successfully imported into Firefox.</p>	<p>1.1 Long-lived DV certificates Certs are IV/OV, not DV</p> <p>1.2 Wildcard DV SSL certificates Certs are IV/OV, not DV</p> <p>1.3 Issuing end entity certificates directly from roots No</p> <p>1.4 Allowing external entities to operate unconstrained subordinate CAs No</p> <p>1.5 Distributing generated private keys in PKCS#12 files No</p> <p>1.6 Certificates referencing hostnames or private IP addresses No</p> <p>1.7 OCSP Responses signed by a certificate under a different root No</p> <p>1.8 CRL with critical CIDP Extension Successfully downloaded the FhG employee CRL into Firefox.</p>
<p>If the root CA audit does not</p>	<p>http://pki.telesec.de/service/documents/Audits.zip</p>	

<p>include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/</p>	<p>Annual audits performed by T-Systems.</p> <p>2008 audit statements provided.</p> <p>From Wolfgang: We did this to have formal statements for our contracts, not to have a public statement, so those documents are only available in German.</p>	
<p>Provide information about the CRL update frequency for end-entity certificates. There should be a statement in the CP/CPS to the effect that the CRL for end-entity certs is updated whenever a cert is revoked, and at least every 24 or 36 hours.</p>	<p>Section 4.9.7 of CP: "CRLs must be generated and published at least once a month. If a certificate is revoked, a new CRL must be generated and published without delay."</p>	<p>Section 2.3 of CPS: Soon as revocation occurs. At least once per week.</p>