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**	**Status/Notes**
Root Name	Deutsche Telekom Root CA 2	COMPLETE
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: Deutsches Forschungsnetz, DFN and Fraunhofer Institute	COMPLETE
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.	CP: http://pki.telesec.de/service/documents/T-Systems-Root-CP_en.pdf Service Description: http://pki.telesec.de/service/documents/service-spec_T-Systems-Root-Signing_en.pdf In CP: 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..	In Progress?

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/. 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	T-Systems is updating their Root CP. We will also provide a link to an extension of our Root CP until the end of the week, which describes the handling of external SubCAs (This handling was applied on both SubCAs). This extension will become part of the CP, when the public discussion has finished with no additional or minor requirements.	In Progress?
Whether or not the root CA audit includes the sub-CAs. 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.	T-Systems audit does not include the sub-CAs. Service Description: T-Systems perform yearly audits of the Customer's CA environment to check compliance with the agreed policies. T-Systems provide a publicly accessible revocation service for CA certificates in the form af an "Authority Revocation List (ARL)".	COMPLETE

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**	**Status/Notes**
Sub-CA Company Name	Deutsches Forschungsnetz, DFN	Fraunhofer Institute Fraunhofer Corporate PKI (FhG)	COMPLETE
Sub-CA Corporate URL	http://www.pki.dfn.de	http://www.pki.fraunhofer.de/	COMPLETE
CPS Links	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/Certificate_Policy_Fraunhofer_Corporate_PKI.pdf http://pki.fraunhofer.de/cp/Certification_Practice_Statement_Fraunhofer_Corporate_PKI.pdf	COMPLETE

CA hierarchy under the sub-CA.	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. 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". All CAs at the Global security level are operated by the DFN-Verein.	This sub-CA provides certification services for FhG employees and machines. Within FhG there are two subordinate CA's, one issues end-entity certs for employees, the other for machines.	COMPLETE
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.	IV/OV 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.	IV/OV 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.	COMPLETE
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 objects -- entity submitting the certificate signing request is the same entity referenced in the certificate	Verification of domain ownership: **Not found** Verification of email address ownership: Section 3.2.3 of CP: the e-mail address must be present and checked during in-person registration.	Section 3.2.3 of CPS: the FhG institutes provide the email address and the domain name for the applicant. This SIGMA system contains identity information. Section 3 of the CP: Identification and Authentication. 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. Section 3.2.3 of CP: All FhG employees are registered within the	For DFN, I could not find the text that demonstrates that reasonable measures are taken to verify the domain name ownership/control as per section 7 of http://www.mozilla.org/projects/security/certs/policy/.

		SIGMA system. Services/machines are included in a central list of registered services/machines. Subscribers must be personally present with ID cards and passports.	
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.	1.1 Long-lived DV certificates Certs are IV/OV, not DV 1.2 Wildcard DV SSL certificates Wildcard certs are not permitted as per CP. 1.3 Issuing end entity certificates directly from roots No 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. 1.5 Distributing generated private keys in PKCS#12 files Not found. 1.6 Certificates referencing hostnames or private IP addresses Not found. 1.7 OCSP Responses signed by a certificate under a different root N/A 1.8 CRL with critical CIDP Extension CRLs from http://www.pki.dfn.de/index.php?id=gridcrl successfully imported into Firefox.	1.1 Long-lived DV certificates Certs are IV/OV, not DV 1.2 Wildcard DV SSL certificates Certs are IV/OV, not DV 1.3 Issuing end entity certificates directly from roots No 1.4 Allowing external entities to operate unconstrained subordinate CAs No 1.5 Distributing generated private keys in PKCS#12 files No 1.6 Certificates referencing hostnames or private IP addresses No 1.7 OCSP Responses signed by a certificate under a different root No 1.8 CRL with critical CIDP Extension Successfully downloaded the FhG employee CRL into Firefox.	COMPLETE
If the root CA audit does not			Need recent audit

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/			statements
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.	Section 4.9.7 of CP: "CRLs must be generated an published at least once a month. If a certificate is revoked, a new CRL must be generated and published without delay."	Section 2.3 of CPS: Soon as revocation occurs. At least once per week.	COMPLETE