

TC ROOTSIGNING

Service Description

1. General

TC RootSigning is a root signing service for enterprises that want to issue and manage their own client and SSL certificates.

TC RootSigning allows enterprises to manage their own CA and perform registration authority (RA) functions for the issuance of globally trusted digital certificates (X.509) in their enterprise. The Company CA gains access to the public root of TC TrustCenter.

2. Standard Features

TC RootSigning includes the following deliverables and services:

- A Company CA Certificate which chains to a TC TrustCenter Class 2 Generation II root certificate.
- Enables you to issue privately branded and globally trusted X.509 certificates in your enterprise and to your partners.
- Provision of a 14-day evaluation test certificate.
- Online access to the Root Certificate Revocation List.
- Annual license at an all-inclusive price.

3. REQUIREMENTS AND COMPLIANCE GUIDELINES

To prevent any security compromises caused by malicious intent, system failures or inadvertent errors, customers are required to meet and adhere to guidelines for generating and managing certificates in a trustworthy fashion.

3.1 Organization Eligibility Requirements

The following requirements have to be met by the TC RootSigning customers:

- (a) The customer must maintain a net worth in excess of EUR 3 Mio. or more.
- (b) The customer must maintain an errors and omissions insurance for claims and damages related to its role as CA as well as a comprehensive general liability insurance each in the amount of EUR 2 Mio. or more.
- (c) The customer must provide and maintain a Certificate Practice Statement (CPS) & Certificate Policy Definition (CPD) consistent with industry standards for commercial CAs and conforming to RFC 3647 and ETSI TS 102 042 (or equivalent standard). The CPS/CPD must be compliant to the TC TrustCenter CPS/CPD (see <http://www.trustcenter.de/about/repository.htm>).
- (d) The customer must provide and maintain a Certificate Policy Definition (CPD) consistent with industry standards for commercial CAs and compliant with AICPA WebTrust for CAs audit standard. TC TrustCenter reserves the right to have, at their expense with proper written notice, a 3rd party to conduct an audit on the customer's CPD. The CPD must be compliant to the TC TrustCenter CPD (see <http://www.trustcenter.de/about/repository.htm>).

3.2 CA Eligibility Requirements

- (a) The customer must operate an approved CA product or vendor (e.g. UniCERT, RSA Keon, Microsoft CA, Entrust Authority).
- (b) The customer has to use hardware key generation and storage on a FIPS 140-1 or rather 140-2 level 2 (or appropriate European standard, minimum ITSEC E2 or CommonCriteria EAL3) compliant device.
- (c) The signed CA certificate will be valid for the term of the agreement and can be renewed according to terms of a renewal agreement. The maximum possible validity of a signed CA certificate is limited to the expiration date of the TC TrustCenter root certificate.
- (d) The customer must maintain a CRL for all issued certificates. The CRL shall be updated promptly upon the revocation of a certificate, but in no case shall such update occur more than one (1) business day following revocation. The CRL validity period shall not exceed thirty (30) days. The definite final CRL has to be issued directly before the Company CA Certificate expires.

3.3 Certificate Requirements

- (a) With the signed Company CA Certificate the following X.509 Certificates may be issued in a quantity as specified in Attachment 2:
 - Client Certificates (to be used by a single person)
 - Team Certificates (can be used by a group of persons. For formal reasons it is assigned to the person who is responsible for that group)
 - Function Certificates (dedicated to computers or applications in order to serve special purposes, e.g. mail gateways. For formal reasons it is assigned to a person who is responsible for the proper use of the certificate)
 - SSL Certificates (dedicated to web servers). The customer must be owner of the domains for which the certificates are issued.
- (b) Client, Team and Function Certificates may be issued to employees of the company or subsidiaries. This means the O-field of issued certificates contains either the legal name of the customer or of one of its subsidiaries (majority interest held). The amount of certificates issued to individuals without direct affiliation with the company may not exceed 10% of the total amount of issued certificates.
- (c) Certificates may not be resold or accounted for in any way.
- (d) Certificates can be issued for one or multiple years depending on the term of agreement. The validity of the issued certificates may not exceed the validity of the signed Company CA Certificate.
- (e) Upon reasonable written request the customer has to provide actual and detailed information about the number of certificates issued and the validity period of each certificate.

3.4 Certificate Revocation

To prevent any security compromises caused by malicious intent, system failures or inadvertent errors, customers are required to meet and adhere to guidelines for generating and managing certificates in a trustworthy fashion.

- (a) The customer notifies TC TrustCenter as soon as the suspected compromise is detected.
- (b) On their letterhead the customer faxes a signed letter requesting TC TrustCenter to revoke the signed Company CA Certificate.
- (c) TC TrustCenter revokes the respective Company CA Certificate.

4 TC ROOTSIGNING SETUP

Prior to issuing a signed Company CA Certificate the following information has to be provided:

- (a) A main technical contact at customer's side who will be acting as the Point of Contact (POC).
- (b) A Customer Support Contact (CSC) who, in the event a subscriber mistakenly contacts TC TrustCenter for support, can be contacted.
- (c) The certificate profiles of the X.509 certificates the company CA is supposed to issue. These profiles will be reviewed and approved by TC TrustCenter.
- (d) The completed TC RootSigning Certificate Enrollment Form which includes all arbitrary CA certificate parameters.
- (e) The PKCS#10 request

The CA certificate will be delivered in a PEM encoded file.

Typically the request used for the initial evaluation test certificate is also used for the issuing of the productive Company CA Certificate. In exceptional cases as the CA software does not allow importing a CA certificate without a further request, TC TrustCenter accepts a new request.