



You are here: [Homepage](#) [Publications](#) [Technical Guidelines](#) **BSI TR-03145 Secure Certification Authority operation**

BSI TR-03145 Secure Certification Authority operation

The business of Public Key Infrastructures (PKI) is a business of trust. A PKI is used either to keep information secret or to determine the authenticity and integrity of information. This requires that the Certification Authorities (CAs) running the PKI itself are trustworthy and trusted by the relying parties.

To achieve trust, two conditions have to be fulfilled. At first a basis has to be built which legitimates the trust. This is achieved by the CA implementing organizational and technical security measures for an appropriate security level and defining rules for all entities participating in a PKI.

In a second step the deployment of the security measures has to be documented in a transparent way, to build trust with potential customers. That can be achieved by passing an audit based on clear and documented requirements.

This TR aims to support CAs on both steps, as it defines requirements for Certificate Authorities for implementing secure CA operation and it builds a basis for a audit and certification process.



[BSI TR-03145 Secure Certification Authority operation \(pdf, 2.54 MB\)](#)

© Federal Office for Information Security (BSI). All rights reserved