Federal Office
for Information Security

Technical Guideline BSI TR-03145 Secure CA Operation

Part 5: Specific requirements for a Public Key Infrastructure for Technical Security Systems

Version 1.0.0
2023-03-09

Document history

Version	*Date*	*Description*
1.0.0	2023-03-09	Initial Version

Table 1: Version history

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn

E-Mail: registrierkassen@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

With the digital transformation of business processes and the increasing use of Electronic Record-keeping Systems, business transactions are increasingly represented and recorded digitally. In order to prevent subsequent manipulation of these digital records, their integrity, authenticity and completeness must be ensured. This is achieved by using a Technical Security System (TSS). The TSS manages the recording and securing of these digital records. Fiscal authorities can request these records and check them with respect to completeness, correctness, and authenticity.

Integrity and authenticity are implemented by means of digital signatures and a Public Key Infrastructure (PKI). I.e. the TSS signs the digital records with its private key. The corresponding public key is bound to the signing TSS by means of a certificate which is issued by a Certification Authority (CA). In general, PKIs are hierarchically organized as follows: The Root CA is the topmost instance of a PKI and the trust anchor within a PKI. The Root CA defines rules and checks the compliance with these rules. Additionally, the Root CA signs and issues Sub CA certificates and thus, expresses its trust in these Sub CAs. Within a TSS PKI, a Sub CA signs and distributes certificates for end entities. In the given application context, the end entities are TSS.

This document is part 5 of the Secure CA operation series of [BSI TR-03145]. Part 1 [BSI TR-03145-1] of the document series compiles “Generic Requirements for Trust Centers instantiating as Certification Authoritiy (CA) in a Public-Key Infrastructure (PKI) with a security level ‘high’”. The present part 5 of [BSI TR-03145] defines secure operation requirements for Certification Authorities within a Public Key Infrastructure for TSS.

Requirements for TSS are defined in [TR-03153] and are not part of this document.

1.1 Scope and structure of this document

This document concerns all Certification Authorities within a PKI for TSS and defines specific requirements for PKIs in the given application context. The requirements in this document [BSI TR-03145-5] supplement the general requirements defined in [BSI TR-03145-1]. Therefore all requirements defined in [BSI TR-03145-1] SHALL be completely fulfilled by all Certification Authorities in a PKI for TSS, unless explicitly stated otherwise in this document.

In the context of the implementation of a TSS Public Key Infrastructure, the following documents are relevant:

- [BSI TR-03153-1] This Technical Guideline defines binding requirements for securing digital records by means of a TSS.
- [BSI TR-03151-1] This Technical Guideline specifies the Secure Element Application Programming Interface (SE API) that allows standardized access to security functionalities in order to secure authenticity and integrity of information by creating digital signatures over them.
- [BSI TR-03145-1] This Technical Guideline denotes general requirements for a secure CA operation and is refined and supplemented by the Technical Guideline at hand.
- [BSI TR-03116-5] This Technical Guideline profiles the cryptographic requirements reflecting the algorithms and key lengths recommend for TSS.

The present document refines and or extends the requirements of [BSI TR-03145-1] and, if relevant for TSS PKI operators, accordingly references [BSI TR-03153-1], [BSI TR-03151-1] or [BSI TR-03116-5].

This document is structured as follows:

- Chapter 2 provides a general overview of the entities of a Public-Key Infrastructure for TSS and the relying parties.

- Chapter 3 details requirements concerning the identification and registration of TSS manufacturer and the personalization of TSS.
- Chapter 4 describes requirements specific to Certification Authorities in a TSS Public-Key Infrastructure and mainly follows the structure of [BSI TR-03145-1].
- Chapter 5 describes general requirements for a TSS Public-Key Infrastructure and also mainly follows the structure of [BSI TR-03145-1].
- Chapter 6 determines requirements for the interoperability, especially with respect to the fiscal inspection of digital records.

1.2 Keywords

Within this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC 2119] when, and only when, they appear in all capitals, as shown here.

1.3 Abbreviations

The abbreviations and definition of terms that are relevant in this document are given below.

Abbreviation	***Definition***
BMF	Federal Ministry of Finance (German: Bundesministerium der Finanzen)
BSI	Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik)
CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation Lists
CSR	Certificate Signing Request
TSS	Technical Security System
PKI	Public Key Infrastructure