



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI•**

BSI-TR-03109 - Dachdokument

# Technische Richtlinie BSI TR-03109

Version 1.1

Datum:2021-09-22, Commit:9127ecf6



Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

E-Mail: [smartmeter@bsi.bund.de](mailto:smartmeter@bsi.bund.de)

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2021

# Inhaltsverzeichnis

1.	Einleitung .....	1
2.	Aufbau der Technischen Richtlinie .....	2
3.	Komponenten im intelligenten Messsystem .....	4
3.1.	Smart-Meter-Gateway .....	4
3.2.	Sicherheitsmodul .....	4
3.3.	Kryptografische Vorgaben .....	5
3.4.	Smart-Metering-PKI .....	5
3.5.	Weitere Systemeinheiten .....	6
3.6.	Administration und Betrieb .....	6
	Literaturverzeichnis .....	7



# 1. Einleitung

Die Technische Richtlinie (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Titel „Technische Richtlinie BSI-TR-03109“ beschreibt die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Komponenten im Umfeld des Smart Metering erfüllen müssen in prüfbarer Art und Weise.

Die TR ist modular aufgebaut und referenziert auf die komponentenspezifischen Module.

## 2. Aufbau der Technischen Richtlinie

Die Technische Richtlinie BSI-TR-03109 umfasst die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die Einzelkomponenten in einem Smart Metering System erfüllen müssen. Die Technische Richtlinie definiert abschließend alle Anforderungen an die jeweilige Einzelkomponente. Insofern Konformitätsbewertungsverfahren ("TR-Zertifizierungen") zu Einzelkomponenten in einem Smart Metering System durchgeführt werden sollen, beschreibt eine Testspezifikation zur jeweiligen Technischen Richtlinie Details zur Durchführung von Prüffällen und zur Akzeptanz von Prüfevidenzen auf Basis der BSI-Zertifizierungs- und -Anerkennungsverordnung (BSIZertV). Testspezifikationen zur TR-03109 sind kein Bestandteil der Technischen Richtlinie, werden in diesem Dokument jedoch zur besseren Übersicht mit aufgeführt.



Abbildung 2.1. Dokumentenstruktur der TR-03109

## 3. Komponenten im intelligenten Messsystem

Die folgenden Abschnitte listen die Anforderungsdokumente in Form von Technischen Richtlinien des BSI zu den Einzelkomponenten im intelligenten Messsystem auf. Insofern Testspezifikationen zu einzelnen Technischen Richtlinien bestehen oder geplant sind, werden diese zur besseren Übersicht unterhalb der jeweiligen Anforderungsdokumente benannt.

### 3.1. Smart-Meter-Gateway

#### 3.1.1. TR-03109-1 Technische Richtlinie - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems



##### Status

Veröffentlicht in Version 1.1 vom 17.09.2021

Die Technische Richtlinie TR-03109-1 stellt Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, kurz Smart-Meter-Gateway. Sie referenziert und ergänzt das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems, indem die funktionalen Sicherheitsanforderungen an diese Komponente und ihre Einsatzumgebung erweitert werden.

Sicherheitstechnische Anforderungen an das Smart Meter Gateway werden durch das Common Criteria-Schutzprofil [PP-0073] definiert.

#### 3.1.2. Testspezifikation zur TR-03109-1



##### Status

Dokument in Vorbereitung

Die Testspezifikation definiert, basierend auf der Technischen Richtlinie TR-03109-1, Prüffälle für die Interoperabilitätseigenschaften und dient somit als Prüfgrundlage zur Evaluierung und anschließenden TR-Zertifizierung des Smart-Meter-Gateways.

### 3.2. Sicherheitsmodul

#### 3.2.1. TR-03109-2 Technische Richtlinie - Anforderungen an die Interoperabilität des Sicherheitsmoduls



##### Status

Veröffentlicht in Version 1.1 vom 15.12.2014

In der TR-03109-2 wird die Funktionalität des Sicherheitsmoduls für das Smart-Meter-Gateway spezifiziert. Das Sicherheitsmodul bildet eine zentrale Sicherheitskomponente, die zum einen als sicherer Schlüsselspei-



cher für das Gateway dient und zum anderen wesentliche kryptographische Routinen (im Bereich asymmetrischer Kryptographie) für das Gateway bereitstellt.

Sicherheitstechnische Anforderungen an das Sicherheitsmodul werden zudem durch das Common Criteria-Schutzprofil [PP-0077] festgelegt.

### 3.2.2. Testspezifikation zur TR-03109-2



#### Status

Veröffentlicht in Version 1.0 vom 06.03.2018

Die Testspezifikation definiert, basierend auf der Technischen Richtlinie TR-03109-2, Prüffälle für die Interoperabilitätseigenschaften und dient somit als Prüfgrundlage zur Evaluierung und anschließenden TR-Zertifizierung des Sicherheitsmoduls des Smart-Meter-Gateways.

## 3.3. Kryptografische Vorgaben

### 3.3.1. TR-03109-3 Technische Richtlinie - Kryptografische Vorgaben für die Infrastruktur von Messsystemen



#### Status

Veröffentlicht in Version 1.1 vom 17.04.2014

Die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren für die Infrastruktur von Messsystemen werden in der TR-03109-3 beschrieben. Basierend auf den Technischen Richtlinien [TR-02102-1] und [TR-03111] werden in diesem Dokument verbindlich die einzusetzenden kryptographischen Verfahren und Primitive sowie zu verwendenden Schlüssellängen für die Absicherung der Infrastruktur von Messsystemen vorgegeben.

## 3.4. Smart-Metering-PKI

### 3.4.1. TR-03109-4 Technische Richtlinie - Public Key Infrastruktur für Smart-Meter-Gateways



#### Status

Veröffentlicht in Version 1.2.1 vom 09.08.2017

In der TR-03109-4 wird die Architektur der Smart Meter – Public Key Infrastruktur (SM-PKI) spezifiziert. Die PKI bildet die Grundlage zur Absicherung der WAN-Kommunikation zwischen den Teilnehmern der Smart Meter Gateway Infrastruktur. Hierbei wird über die PKI die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel sichergestellt.

Des Weiteren werden in dieser Technischen Richtlinie die Mindestanforderungen an die Interoperabilität und die Sicherheit der SM-PKI aufgestellt, die in der Zertifizierungsrichtlinie (Certificate Policy, CP) für die SM-PKI berücksichtigt werden müssen. Ferner werden die Profile für die einzusetzenden Zertifikate und Sperrlisten spezifiziert.

## 3.5. Weitere Systemeinheiten

### 3.5.1. TR-03109-5 Technische Richtlinie: Anforderungen an weitere Systemeinheiten des intelligenten Messsystems



#### Status

Dokument in Vorbereitung

### 3.5.2. Testspezifikation zur TR-03109-5



#### Status

Dokument in Vorbereitung

## 3.6. Administration und Betrieb

### 3.6.1. TR-03109-6 Technische Richtlinie - Smart-Meter-Gateway-Administration



#### Status

Veröffentlicht in Version 1.0 vom 26.11.2015

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart-Meter-Gateway-Administrator (GWA) verantwortlich. Die Anwendungsfälle des GWA sind in der TR-03109-6 auf Basis der TR-03109-1 definiert.

Um diesen Betrieb verantwortungsvoll, zuverlässig und sicher gewährleisten zu können, muss der IT-Betrieb beim GWA Mindestanforderungen genügen. Die TR-03109-6 definiert geeignete und angemessene Mindestanforderungen an die Informationssicherheit für diesen Bereich des GWA.

## Literaturverzeichnis

- [PP-0073] *BSI-CC-PP-0073-2014, v1.3 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. 2014 . Bundesamt für Sicherheit in der Informationstechnik
- [PP-0077] *BSI-CC-PP-0077-2014, v1.3 Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)*. 2014 . Bundesamt für Sicherheit in der Informationstechnik
- [TR-02102-1] *BSI TR-02102-1: Kryptographische Verfahren und Schlüssellängen*. Jährlich aktualisiert . Bundesamt für Sicherheit in der Informationstechnik
- [TR-03111] *Technische Richtlinie BSI-TR-03111 v2.10 Elliptic Curve Cryptography*. 2018 . Bundesamt für Sicherheit in der Informationstechnik

