



Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie

BSI TR-03109

Version 1.0.1, Datum 11.11.2015



Änderungshistorie

Version	Datum	Beschreibung
1.0	18.03.2014	Initiale Version 1.0
1.0.1	11.11.2015	Neues Kapitel 3.6

Inhaltsverzeichnis

	Änderungshistorie.....	2
1	Einleitung.....	7
2	Aufbau der Technischen Richtlinie.....	8
3	Komponenten.....	9
3.1	Smart Meter Gateway – Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.....	9
3.1.1	TR-03109-1 Technische Richtlinie.....	9
3.1.2	TR-03109-TS-1 Testspezifikation.....	9
3.2	Sicherheitsmodul – Anforderungen an die Interoperabilität des Sicherheitsmoduls.....	9
3.2.1	TR-03109-2 Technische Richtlinie.....	9
3.2.2	TR-03109-TS2 Testspezifikation.....	9
3.3	TR-03109-3 Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von Messsystemen.....	10
3.4	TR-03109-4 Public Key Infrastruktur für Smart Meter Gateways.....	10
3.5	Kommunikationsadapter.....	10
3.5.1	TR-03109-5 Technische Richtlinie.....	10
3.5.2	TR-03109-TS-5 Testspezifikation.....	10
3.6	TR-03109-6 Smart Meter Gateway Administration.....	10
	Literaturverzeichnis.....	11
	Stichwort- und Abkürzungsverzeichnis.....	12

Abbildungsverzeichnis

Tabellenverzeichnis

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, sowie die Anforderungen zur Prüfung dieser Eigenschaften.

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. Darüber hinaus werden die Anforderungen zur Prüfung dieser Eigenschaften definiert.

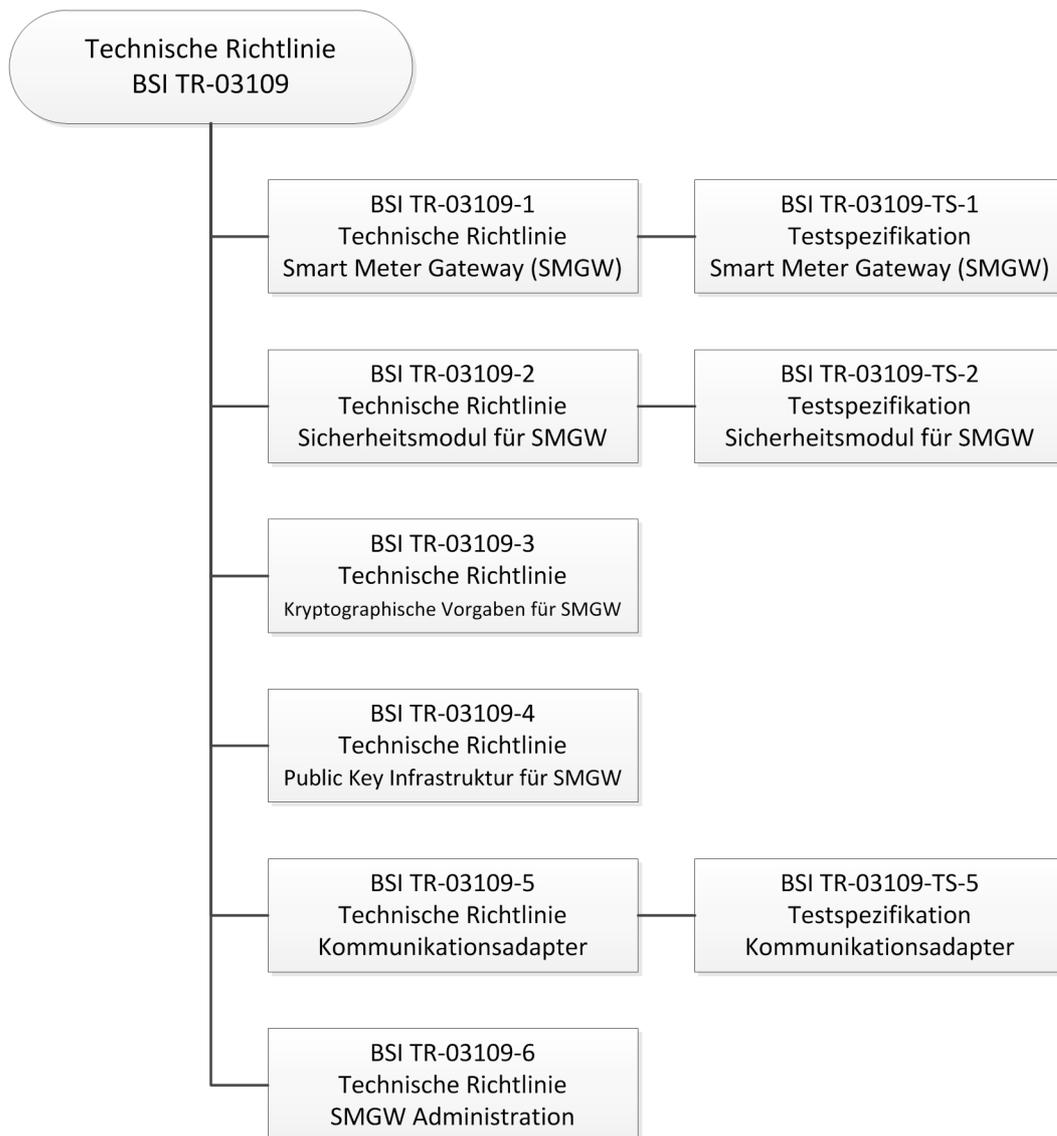


Abbildung 2.1: Dokumentenstruktur der TR-03109

3 Komponenten

3.1 Smart Meter Gateway – Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

3.1.1 TR-03109-1 Technische Richtlinie

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 [SMGW-PP] definiert.

3.1.2 TR-03109-TS-1 Testspezifikation

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 – Anforderungen an die Interoperabilität des Sicherheitsmoduls

3.2.1 TR-03109-2 Technische Richtlinie

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 Schlüsselspeicher 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 [SM-PP] festgelegt.

3.2.2 TR-03109-TS-2 Testspezifikation

Status: Dokument in Vorbereitung

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 TR-03109-3 Kryptographische Vorgaben – Kryptographische Vorgaben für die Infrastruktur von Messsystemen

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 [TR-02102] und TR-03111 [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 TR-03109-4 Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways

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 Kommunikationsadapter

Status: Dokumente in Vorbereitung

3.5.1 TR-03109-5 Technische Richtlinie

3.5.2 TR-03109-TS-5 Testspezifikation

3.6 TR-03109-6 Smart Meter Gateway Administration

Für den sicheren, technischen Betrieb des intelligenten Messsystems ist der Smart Meter Gateway Administrator (SMGW Admin) verantwortlich. Die Anwendungsfälle des SMGW Admin 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 SMGW Admin Mindestanforderungen genügen. Die TR-03109-6 definiert geeignete und angemessene Mindestanforderungen an die Informationssicherheit für diesen Bereich des SMGW Admin.

Literaturverzeichnis

- [SMGW-PP] BSI-CC-PP-0073, Protection Profile for the Gateway of a Smart Metering System (Smart Metering Gateway PP)
- [SM-PP] BSI-CC-PP-0077, Protection Profile for the Security Module of a Smart Metering System (Security Module PP)
- [TR-02102] BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- [TR-03111] BSI TR-03111, Elliptic Curve Cryptography(ECC)
- [TR-03109] BSI TR-03109, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Stichwort- und Abkürzungsverzeichnis