Wie „vertrauen“ sich die Teilnehmer in der iMSys-Infrastruktur? TR-03109 und §52 MSB-G

WAGO Smart-Grid-Fachtagung 2016

Peter Thanisch

VORWEG GEHEN

Inhalt

- Verschlüsselung und Authentifizierung „im digitalen Kosmos“ digitale Zertifikate
- Die digitalen Zertifikate „für die Steuerbox“
- Die digitalen Zertifikate für die Kommunikation zwischen den **E**xternen **M**arkt **T**eilnehmern im Sinne §52 MSB-G

Inhalt

- Verschlüsselung und Authentifizierung „im digitalen Kosmos“ digitale Zertifikate
- Die digitalen Zertifikate „für die Steuerbox“
- Die digitalen Zertifikate für die Kommunikation zwischen den Externen Markt Teilnehmern im Sinne §52 MSB-G

Der SMGW-Admin benötigt komplexe Kommunikations-Strukturen …

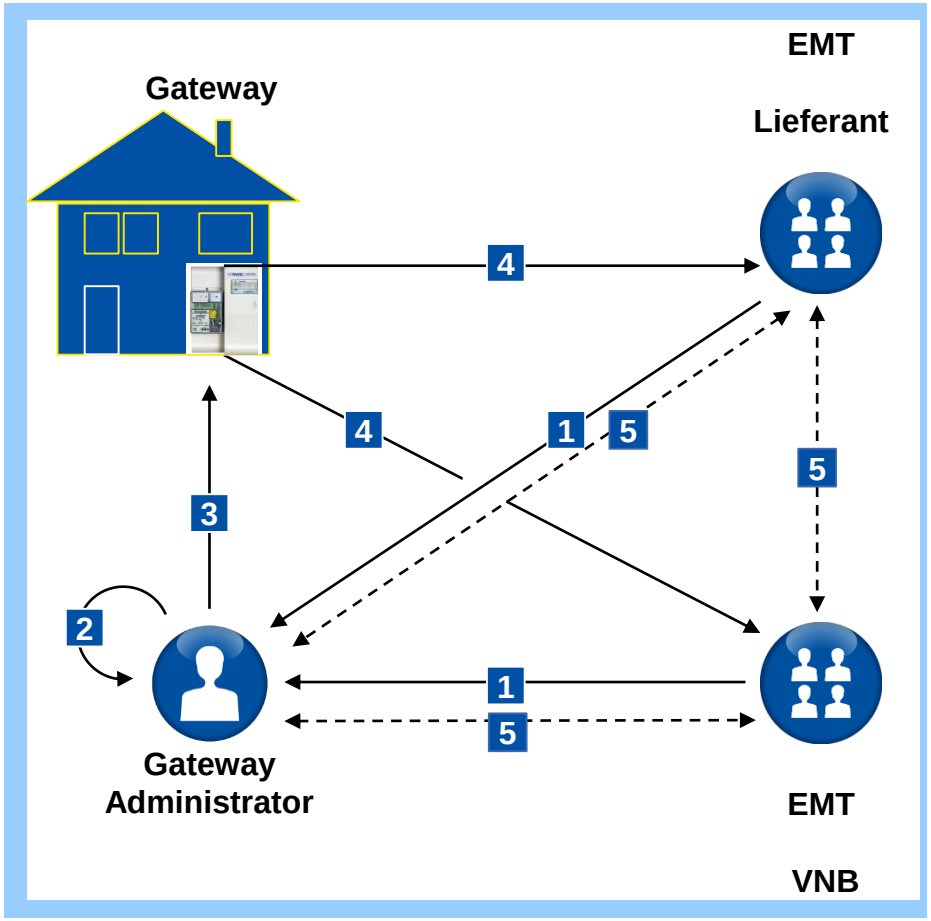


Abbildung entspr. der Szenarien 2 u. 3 der BDEW Kommunikationsszenarien

Erläuterungen der Kommunikationsbeziehungen

1 ➢ Auftrag vom EMT (VNB, Lieferanten, Sonst.), Informationen (Art, Menge, Zeitpunkt der Lieferung) vom Gateway zu erhalten oder Verbindung SMGW ←→ EMT bereit zu stellen.

2 ➢ Betrieb beim SMGW-Admin

- > Prüfen der Berechtigung des EMT (VNB, Lieferanten
- > Aufspielen von Firmware Updates und Profilen (Einbringen der Information vom EMT)

3 ➢ Wake-Up-Signal z. B. für ad-hoc-Anfragen

4 ➢ Versand vorher definierter Informationen an den EMT (z.B. Lieferant oder VNB) oder Aufbau der Verbindung f. Schalthandlungen

5 ➢ Klassische Marktkommunikation gemäß GeLi Gas und GPKE (Formate, Fristen, Prozesse)

… die Verschlüsselung und Authentifizierung untereinander gewährleisten. Einige Fragen

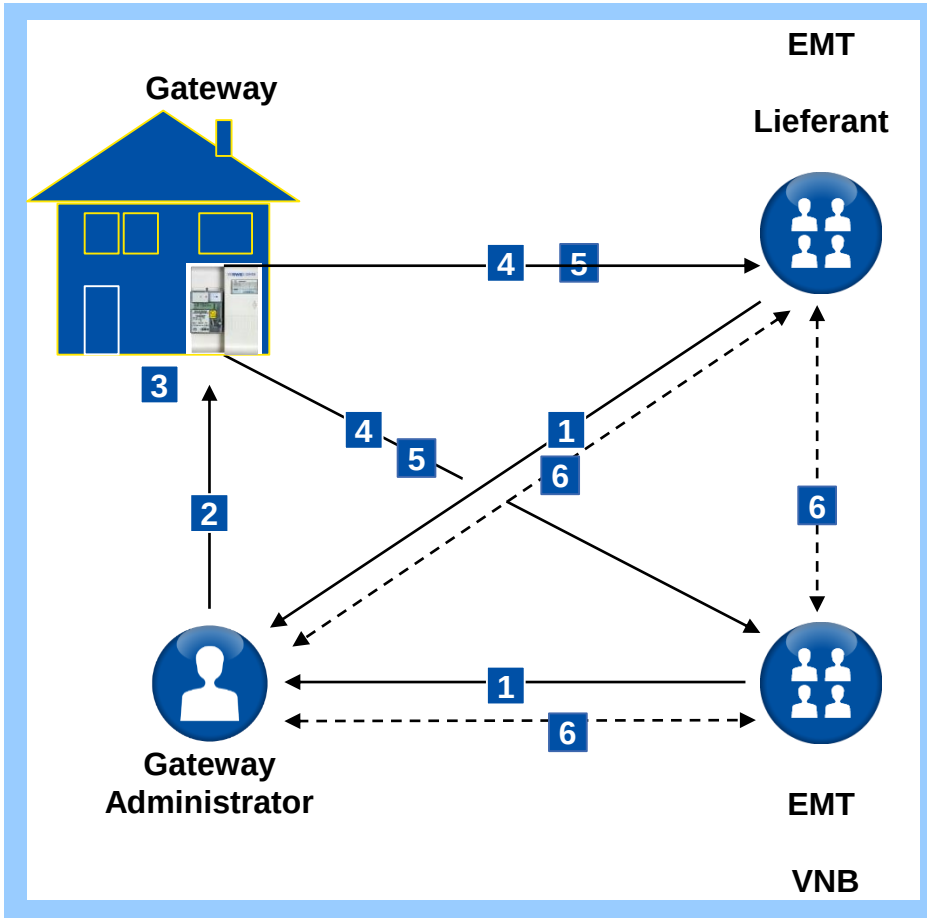
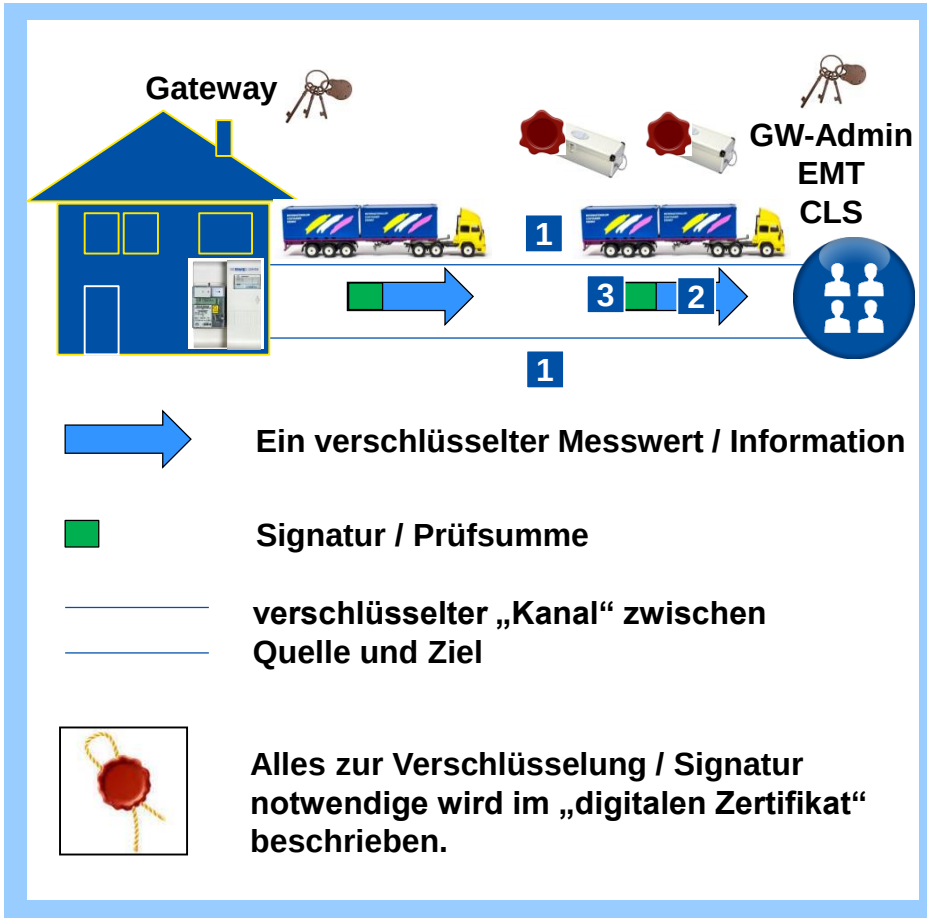


Abbildung entspr. der Szenarien 2 u. 3 der BDEW Kommunikationsszenarien

Fragen an die Teilnehmer im iMSys-Verbund

1. Woher weis der EMT, dass der adressierte SMGW-Admin der ist, den dieser vorgibt zu sein?
2. Woher weis der SMGW-Admin, dass das SMGW dasjenige ist, welches er erreichen will (und nicht ein „böses“?
3. Wie ist gewährleistet, dass die Geräte am SMGW nicht „aus böser Absicht“ ausgetauscht werden?
4. Woher weis das SMGW, ob der adressierte EMT der berechtigte (also richtige) EMT ist?
5. Wie verschlüsselt das SMGW die übertragenen Daten so, dass nur der adressierte EMT diese verstehen kann?
6. Wie verschlüsselt der EMT/SMGW-Admin seine Nachricht, dass nur der berechtigte Empfänger diese Nachricht interpretieren kann?

Etwas zur Verschlüsselung und Authentifizierung in Umfeld des iMSys.



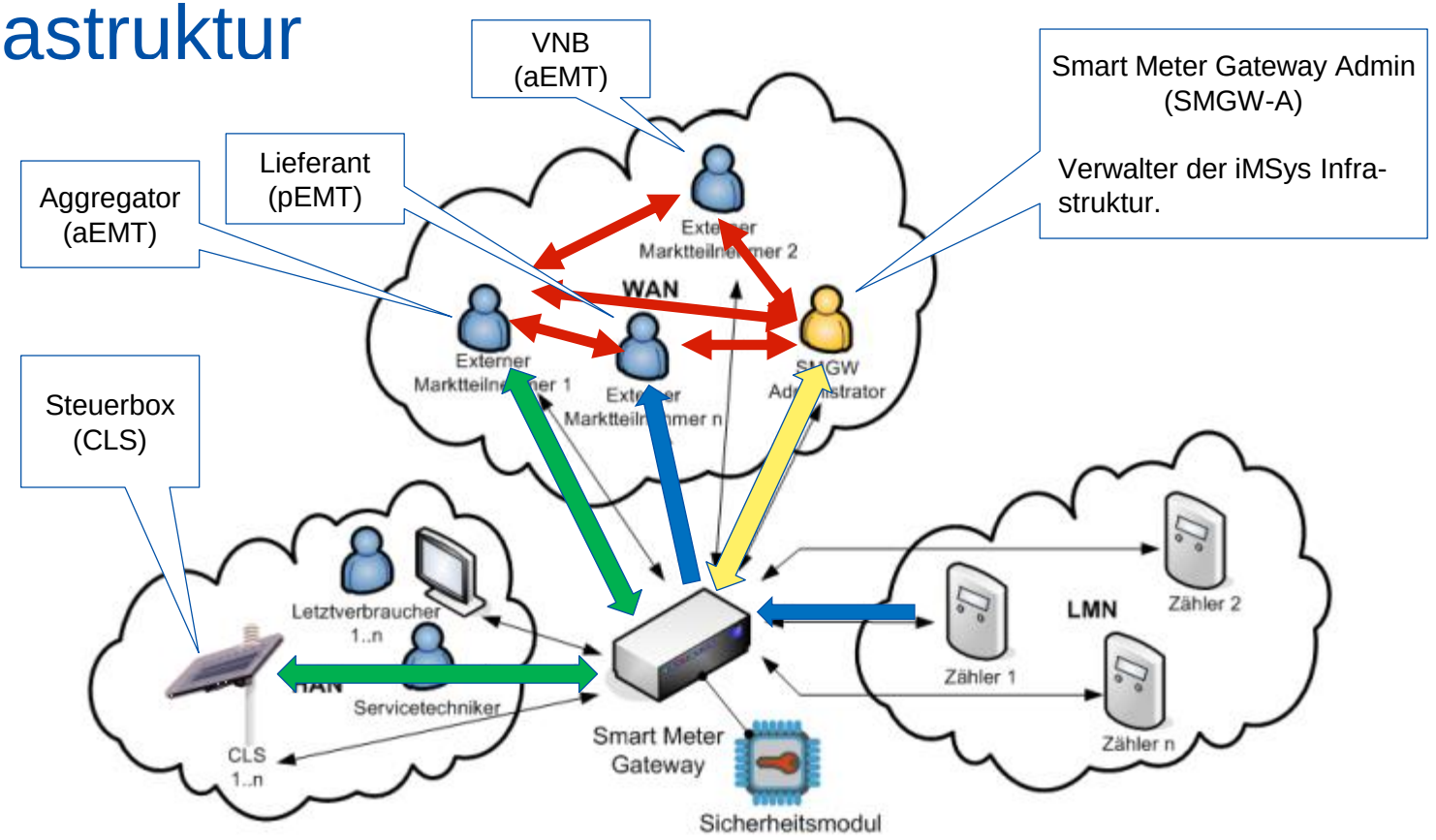
Gleiche (Kommunikations-) Regeln für „alle“

1
- Von der Quelle zum Ziel wird ein verschlüsselter „Kanal“ aufgebaut. Dies soll „Abhören“ verhindern.

2
- Ein Wert/Information, der von der Quelle zum Ziel übertragen werden soll, wird zusätzlich verschlüsselt. Damit ist dieser Wert auch bei Einbruch in den verschlüsselten Kanal gesichert

3
- Der verschlüsselte Wert 2 im verschlüsselten Kanal 1 wird von der Quelle zusätzlich mit einer Prüfsumme 3 abgesichert. Der Wert wird „signiert“. Durch Analyse dieser Signatur / Prüfsumme kann im Ziel festgestellt werden, ob der verschlüsselte Wert auf dem Weg zwischen Quelle und Ziel manipuliert wurde.
- Auch der Rückweg wird analog gesichert: in einem verschlüsselten Kanal werden verschlüsselte Informationen mit zusätzlicher Signatur übertragen.
- Herausgabe-Stelle für diese „digitalen Zertifikate“ ist die „Certification- Authority“ (CA) der Smart Meter Public Key Infrastructure (SM-PKI)

Wer kommuniziert mit wem wie in der iMSys Infrastruktur



Ref: TR03109-4

Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Die Kommunikation ←→ / → / → via SM-GW nach TR-03109-4
Die Kommunikation ⟷ nach §52 (1), (2), (4) MSB-G Entwurf

Die digitalen Zertifikate in der iMSys Infrastruktur

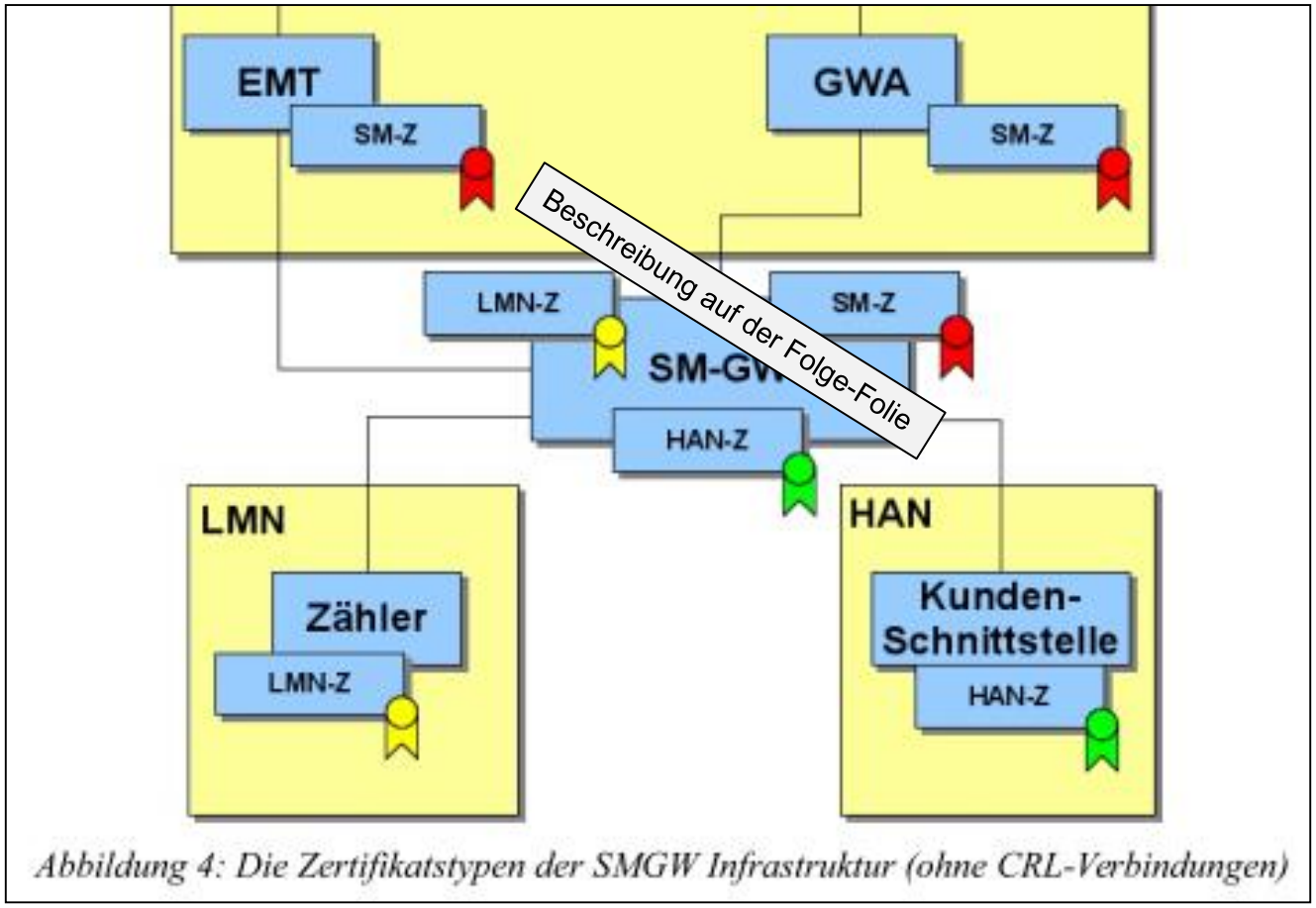


Abbildung 4: Die Zertifikatstypen der SMGW Infrastruktur (ohne CRL-Verbindungen)

Ref: TR03109-4

Spezifikation der digitalen Zertifikate für die iMSys Infrastruktur

2.6.1 Smart Metering-Zertifikate
Die Smart Metering-Zertifikate (SM-Z, rot markiert) werden zur Kommunikation mit dem SMGW über die WAN-Schnittstelle verwendet. Des Weiteren werden die Zertifikate zur Absicherung der Kommunikation über die Web-Service-Schnittstelle und mit den Verzeichnisdiensten verwendet. Die Zertifikate können auch zur Absicherung der Kommunikation zwischen den Endnutzern verwendet werden.
Diese Zertifikate sind Gegenstand dieser Spezifikation. → **TR-03109-4**

2.6.2 LMN-Zertifikate (informativ)
LMN-Zertifikate (LMN-Z, gelb markiert) können optional zur gegenseitigen Authentisierung von Zählern und SMGW im Local Metrological Network (LMN) verwendet werden. Die Zertifikate sind selbst-signiert und stammen nicht aus der SM-PKI.
Das Zertifikatsprofil und die weiteren Anforderungen an die LMN-Zertifikate werden in [2] festgelegt. Die zugehörigen kryptografischen Anforderungen werden in Abschnitt 6 in [6] definiert.
Bundesamt für Sicherheit in der Informationstechnik Architektur der SM-PKI → **hier nicht betrachtet**

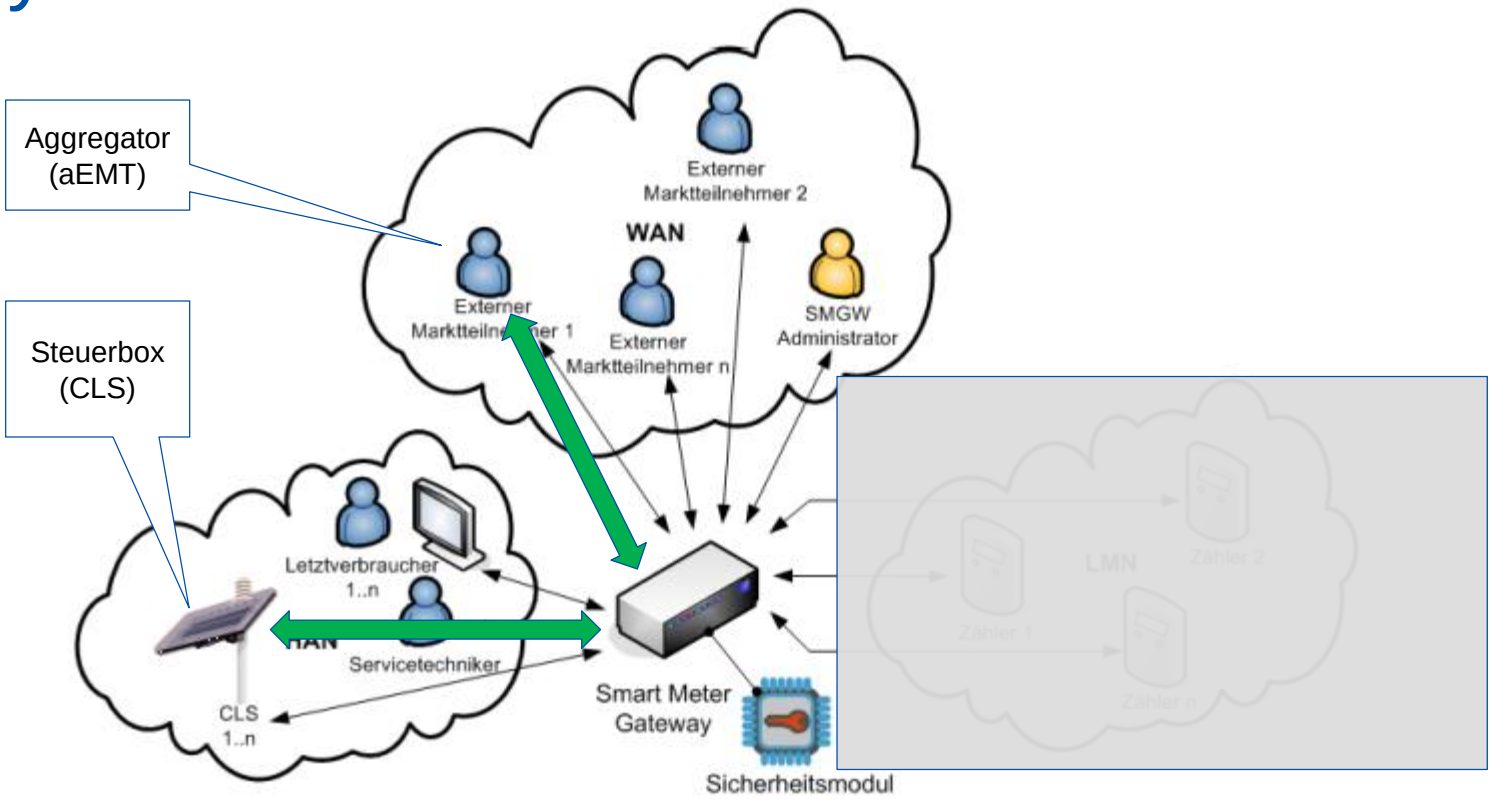
2.6.3 HAN-Zertifikate (informativ)
Die HAN-Zertifikate (HAN-Z, grün markiert) können optional zur Authentisierung von Geräten (z.B. Kunden-Schnittstelle) an der HAN-Schnittstelle des SMGW verwendet werden.
Die weiteren Anforderungen an die HAN-Zertifikate werden in [2] festgelegt. → **TR-03109-3** → **TR-03116-3**

Ref: TR03109-4

Inhalt

- Verschlüsselung und Authentifizierung „im digitalen Kosmos“
- Die digitalen Zertifikate „für die Steuerbox“
- Die digitalen Zertifikate für die Kommunikation zwischen den Externen Markt Teilnehmern im Sinne §52 MSB-G

Die CLS - Kommunikation in der iMSys Infrastruktur



Ref: TR03109-4

Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Die Kommunikation ←→ via SM-GW nach TR-03109-4

Technische Spezifikation Steuerbox ←→ EMT

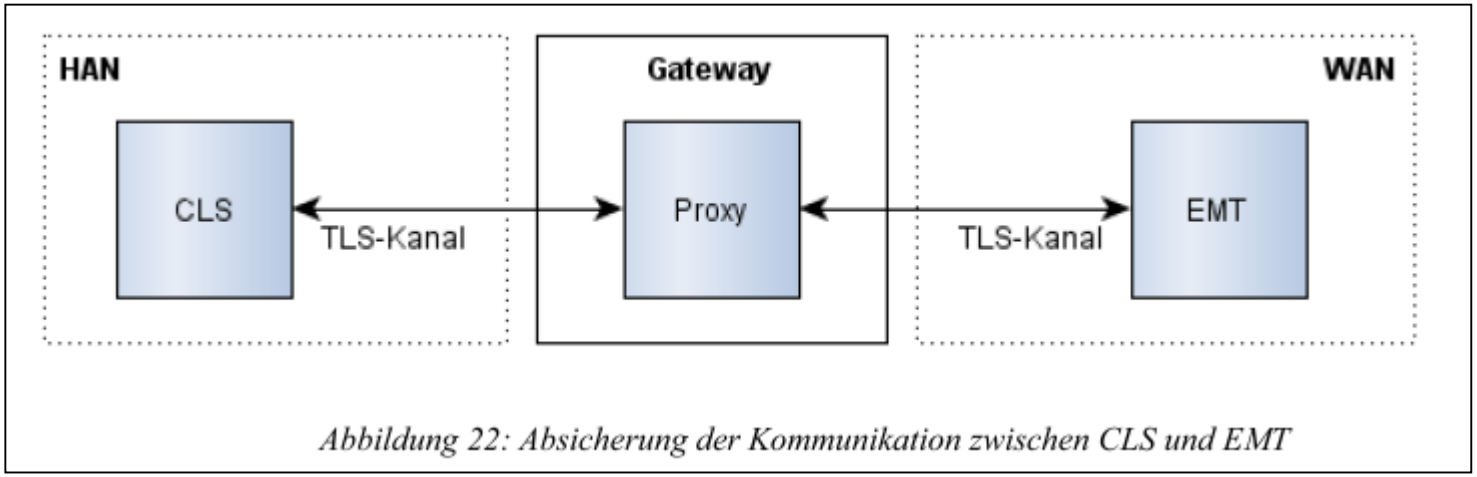


Abbildung 22: Absicherung der Kommunikation zwischen CLS und EMT

Ref: TR03109-4

Absicherung der Kommunikation zwischen Smart Meter Gateway und Teilnehmern im HAN (vgl. [6])	TLS (vgl. Abschnitt 5)

5.1 Migration kryptographischer Verfahren und Schlüssel

Es wird empfohlen, Komponenten im HAN mit der Möglichkeit auszustatten, neue Schlüssel einzuspielen/zu erzeugen und ggf. per Firmware-Update neue kryptographische Verfahren einzuspielen, um so eine weitere Verwendbarkeit der Komponenten auch nach einer erforderlichen Migration kryptographischer Verfahren zu ermöglichen.

Ref: TR03116-3

Vorgabe an die HAN-Zertifikate für die Kommunikaton CLS/Steuerbox ←→ SM-GW

> **3.4.4.3 Identifizierung und Authentifizierung**

> Das SMGW MUSS sicherstellen, dass zur Identifizierung und Authentifizierung von …
> und CLS gegenüber dem SMGW ausschließlich **HAN-Zertifikate** verwendet werden.
> ….
> Das SMGW MUSS sich immer mit seinem **HAN Zertifikat** GW_HAN_TLS_CRT authentifizieren.
> Das SMGW MUSS die clientseitige Identifizierung und Authentifizierung entweder mittels Zertifikat
> und/oder mittels Kennung und Passwort gemäß HTTP Digest Access Authentication [RFC2617]
> durchsetzen.

> Die Benutzeridentitäten (…, CLS und deren Zertifikate bzw.
> Kennung und Passwörter) MÜSSEN auf dem SMGW registriert bzw. konfiguriert werden, damit
> diese vom SMGW als vertrauenswürdig akzeptiert werden. Einem Letztverbraucher KÖNNEN
> durchaus mehrere Zertifikate bzw. Kennungen und Passworte zugeordnet sein (z.B. …, CLS mit Datenzugriff, usw.).

> Die **HAN-Zertifikate** sind selbst-signiert oder sind von einer herstellerspezifischen CA bzw. einer
> eigenen SMGW-Admin CA ausgestellt worden.
> Die Zertifikate MÜSSEN die Kryptoanforderungen aus [BSI TR-03109-3] erfüllen. Details zu den
> Zertifikaten sind in „Anhang C: Zertifikate im HAN“ definiert.

> Anmerkung: die TR-03109-3 referenziert auf die BSI-TR 03116-3 hinsichtlich kryptographischer Vorgaben.

Ref: TR03109-1

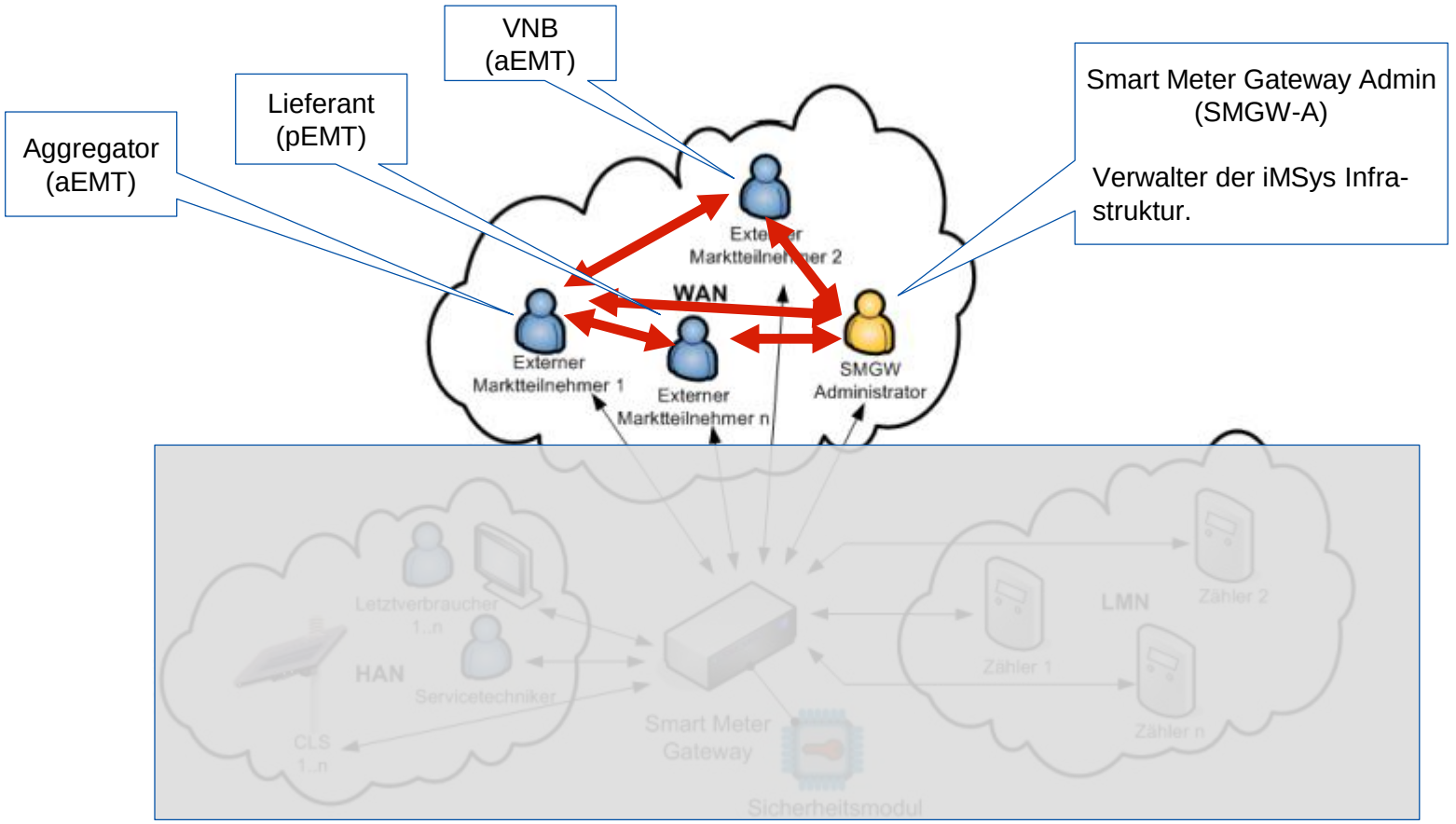
Inhalt

> Verschlüsselung und Authentifizierung „im digitalen Kosmos“

> Die digitalen Zertifikate „für die Steuerbox“

> Die digitalen Zertifikate für die Kommunikation zwischen den **E**xternen **M**arkt **T**eilnehmern im Sinne §52 MSB-G

Nach §52 MSB-G wird die EMT-Kommunikation durch SM-PKI Zertifikate abgesichert.

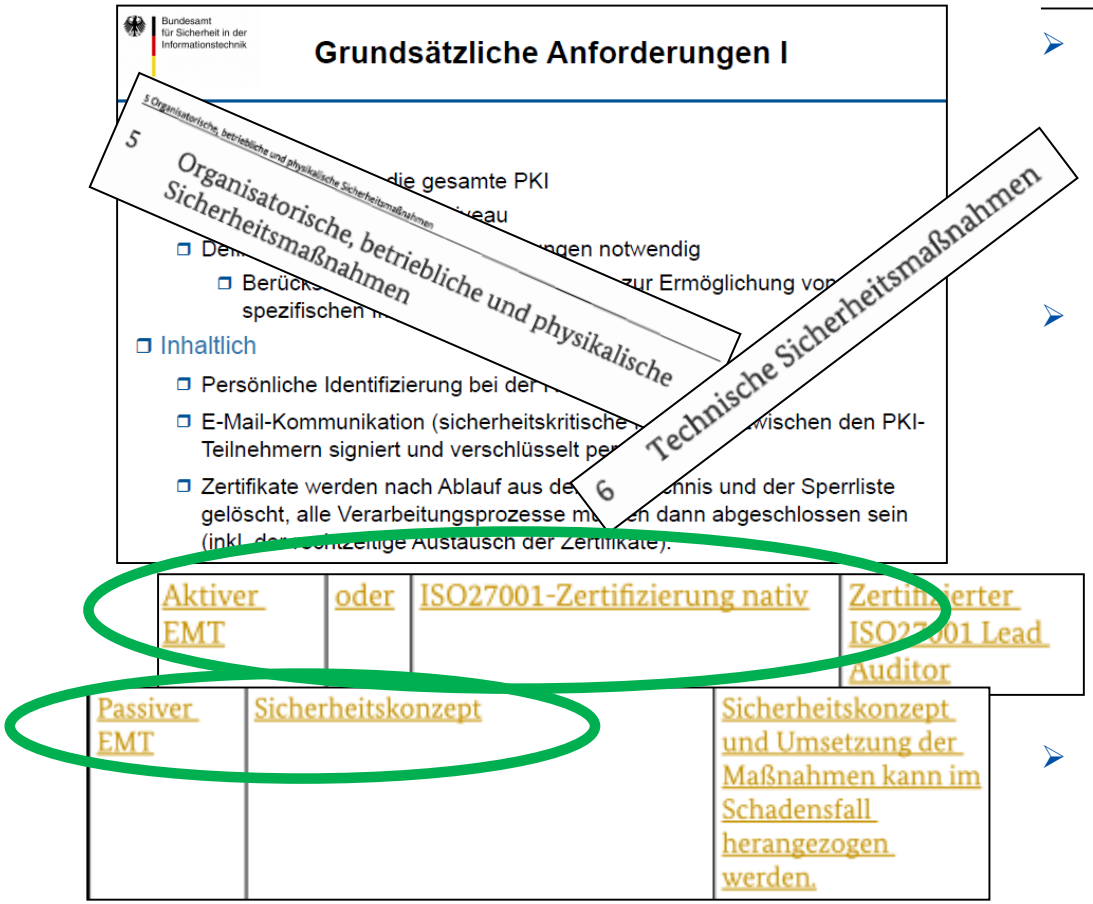


Ref: TR03109-4

Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Die Kommunikation ⟷ nach §52 (1), (2), (4) MSB-G Entwurf

SM PKI CA Forderungen an aktiven und passiven EMT



Erhalt von Zertifikaten ist an Bedingungen geknüpft

- Vorgaben an alle Teilnehmer im Umfeld des iMSys
  - Hersteller
  - SMGW-Admin
  - Aktiver EMT
  - Passiver EMT
- Sicherheitsvorgaben
  - Organisatorische
  - Technische
  - Nachweis eines Sicherheitskonzeptes bei …
    - SMGW-A und aktiver EMT durch **Zertifizierung nach ISO 27001**
    - passiver EMT ggf. Nachweis eines **dokumentierten** Sicherheitskonzept.
- SM-PKI CA in der Version V 1.0.1 seit Ende Mai 2015 gültig. Bisher nur Test-Zertifikate ausgestellt.

Bildquelle: SM-PKI CA,

Vielen Dank für Ihre Aufmerksamkeit
Ihre Fragen?

Peter Thanisch

RWE Deutschland AG
Referent, ISMS-Beauftragter
Kruppstraße 5, 12A01
45128 Essen
T: +49 (201) 12 22117
cert. IT-Systeme Auditor (CISA®)
cert. Datenschutzauditor (TüV Süd)
cert. ISO 27001 Lead Auditor (BSI GmbH)

Lassen Sie uns gemeinsam

VORRWEG GEHEN