dena
Deutsche Energie-Agentur

SET Hub

Leitfaden

Regulatorische Vorgaben für externe Marktteilnehmer (EMT)

Status quo der Anforderungen für die Kommunikation mit intelligenten Messsystemen und die Nutzung der Smart Meter Gateway Infrastruktur in Deutschland

Impressum

Herausgeber:

Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin

Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699

E-Mail: info@dena.de
Internet: www.dena.de

Redaktion:
Tobias Riedel, FZI Forschungszentrum Informatik
Mara Berg, dena

Konzeption & Gestaltung:
The Ad Store GmbH

Stand:
Mai/2024

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2024): „Regulatorische Vorgaben für externe Marktteilnehmer (EMT). Status quo der Anforderungen für die Kommunikation mit intelligenten Messsystemen und die Nutzung der Smart Meter Gateway Infrastruktur in Deutschland“

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Inhalt

1 Grundlegende Einordnung

Die Digitalisierung des Energiesystems ist ein Schlüsselelement für das Gelingen der Energiewende. Durch den Einsatz von digitalen Technologien wird die zunehmende Dynamik, die durch Erneuerbare-Energien-Anlagen und neue flexible Lasten entsteht, besser beherrschbar gemacht. Statt weniger zentraler Kohle- und Gaskraftwerke werden künftig um ein Vielfaches mehr kleine dezentrale Photovoltaik- und Windkraftanlagen Strom produzieren. Gleichzeitig ist davon auszugehen, dass der Strombedarf in den Verteilnetzen durch Wärmepumpen und Elektrofahrzeuge stark ansteigt.

Damit ein zukünftiges Energiesystem effizient und zuverlässig funktioniert, müssen einerseits mehr Daten über die aktuelle Situation der Stromnetze gemessen und kommuniziert werden und andererseits standardisierte und sichere Kommunikationsverbindungen zu den dezentralen Anlagen bestehen. Während es bisher ausreichend war, nur die größeren Verbraucher und Kraftwerke kommunikationstechnisch anzubinden und die Verbräuche von Haushalten und die Leistung kleinerer Photovoltaikanlagen zu schätzen, braucht es in Zukunft eine genauere Datengrundlage. In einem dezentraleren Energiesystem müssen auch Daten kleinteiliger erhoben und verteilt werden. Engpässe sind im Stromnetz zunehmend auf der bislang messtechnisch kaum erfassten Niederspannungsebene zu erwarten, da dort viele Photovoltaikanlagen und neue Lasten wie Wärmepumpen und Ladestationen angeschlossen werden.

Die neuen Lasten sind jedoch oft flexibel und können ihren Strombedarf innerhalb gewisser Grenzen anpassen oder auch in andere Zeitfenster verschieben, je nach Situation im Energiesystem. Darüber hinaus werden zusätzlich zu Photovoltaikanlagen auch dezentrale Batteriespeicher installiert, die ebenfalls einen Beitrag zu einem effizienten und stabilen Energiesystem leisten können. Die Steuerung dieser Anlagen funktioniert entweder über die Anlagen direkt oder indirekt über Energiemanagementsysteme, die basierend auf der Situation im Gebäude, im Netz und am Strommarkt flexible Lasten und Speicher optimiert steuern können. Um über die Situation im Netz informiert zu sein, müssen Energiemanagementsysteme mit den entsprechenden Akteuren und Systemen im Energienetz kommunizieren können, beispielsweise mit Netzbetreibern. Diese wiederum sind ebenfalls auf die Verfügbarkeit von Messdaten hinsichtlich Verbrauch und Erzeugung sowie von Netzzustandsdaten angewiesen, um ihre Netze zu planen und einen effizienten und sicheren Netzbetrieb sicherzustellen.

Die durch diese Kommunikation hinzukommenden Risiken bestehen in potenziellen neuen Cyber-Angriffsflächen im Stromnetz, die durch entsprechende Sicherheitsstandards adressiert werden müssen. Neben der kritischen Infrastruktur der Energieversorgung müssen auch die personenbezogenen Daten von Verbraucherinnen und Verbrauchern zuverlässig geschützt werden.

Für die Nutzung der Flexibilität von kleineren dezentralen Lasten können verschiedene Möglichkeiten in Betracht gezogen werden. Eine Möglichkeit, die Situation im Energiemarkt an flexible Verbraucher zu kommunizieren und gleichzeitig einen Anreiz zu schaffen, darauf zu reagieren, sind dynamische Stromtarife, die sich beispielsweise viertelstündlich ändern. Um sie abrechnen zu können, muss der Stromverbrauch allerdings im Zeitraster der Tarifierung erfasst werden. Die Jahresenergiemenge und die Abrechnung nach dem Standardlastprofil sind dafür nicht ausreichend. Darüber hinaus kann die Visualisierung der Stromverbräuche Verbraucherinnen und Verbrauchern mehr Transparenz hinsichtlich ihres Stromverbrauchs bieten und ihnen Einsparpotenziale aufzeigen.

Um diese genannten Themen, insbesondere die Cybersicherheit und eine granulare Erfassung und einen granularen Versand von Messwerten, zu adressieren, werden intelligente Messsysteme (iMSys) ausgerollt. Dem *Gesetz zum Neustart der Digitalisierung der Energiewende* zufolge sollen ab 2025 für bestimmte Verbraucherinnen und Verbraucher verpflichtend iMSys verbaut werden. Dazu gehören solche mit einem Strombedarf von 6.000 bis 100.000 Kilowattstunden pro Jahr und Verbraucherinnen und Verbraucher mit steuerbaren Verbrauchseinrichtungen (z. B. Ladestationen und Wärmepumpen) nach § 14a EnWG (Energiewirtschaftsgesetz) sowie Erzeuger von 7 bis 100 Kilowatt (z. B. Photovoltaikanlagen). Der Einsatz von iMSys bietet die Möglichkeit, Daten granular zu erfassen, Steuerungssignale zu empfangen, dynamische Tarife abzurechnen und basierend darauf neue Geschäftsmodelle und Anwendungen zu entwickeln.

1.1 Intelligente Messsysteme (iMSys)

Intelligente Messsysteme (iMSys) bestehen aus mindestens einer modernen Messeinrichtung, die Verbräuche eichrechtskonform erfasst und oft als „Smart Meter“ bezeichnet wird, sowie einem Smart Meter Gateway (SMGW) als Kommunikationsschnittstelle. Die moderne Messeinrichtung kann allein noch nicht über das Internet kommunizieren. Das SMGW hat als zentrale Aufgabe, die Kommunikation zwischen den modernen Messeinrichtungen, dem Internet und dem Heimnetz nach spezifischen Sicherheitsanforderungen zu ermöglichen.

Dabei sind aus Sicht des SMGW drei Netzwerke durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert, die in Abbildung 1 dargestellt sind: Das **Wide Area Network (WAN)** umfasst das Internet, aus dem ein externer Marktteilnehmer, wie zum Beispiel ein Stromlieferant oder ein Netzbetreiber, von außen mit dem SMGW in Verbindung treten kann. Das **Home Area Network (HAN)** ist das Heimnetz, das allerdings nicht identisch ist mit dem vorhandenen Heimnetzwerk (LAN/WLAN) der Kunden, sondern ein eigenes lokales Netzwerk darstellt. Darüber können steuerbare Geräte angebunden werden. Alle Zähler des Messstellenbetreibers bei der Verbraucherin oder dem Verbraucher vor Ort (Stromzähler, Gaszähler, Wärmezähler etc.) sind über das **Local Metrological Network (LMN)** mit dem SMGW verbunden.

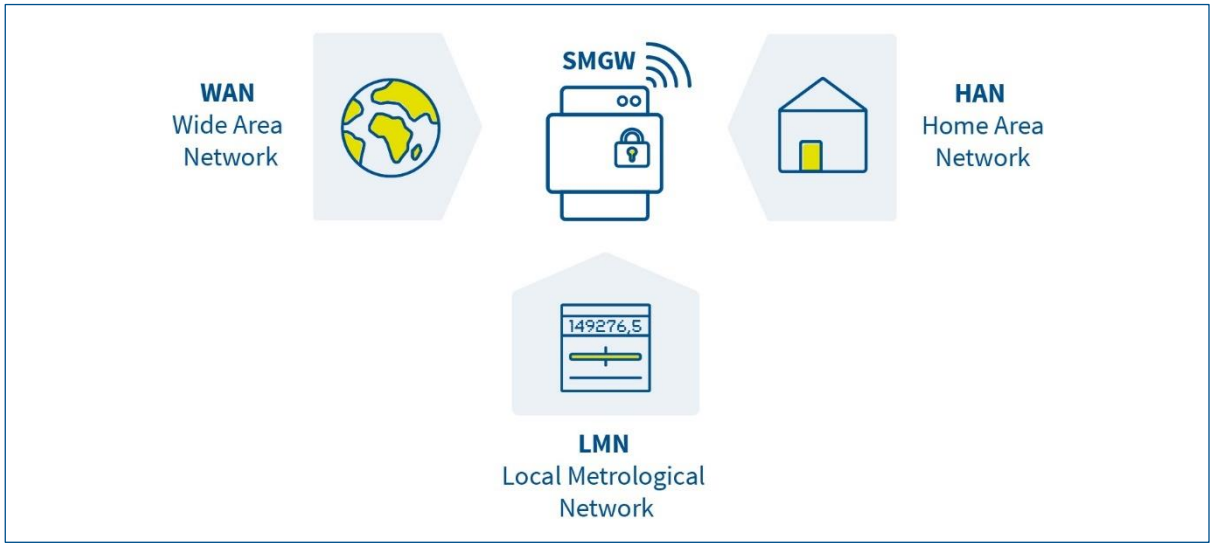

Abbildung 1 Netzwerke des SMGW

Das SMGW ist ein vom BSI standardisiertes Gerät, das auch von diesem zertifiziert wird (vgl. § 24 MsbG (Messstellenbetriebsgesetz)). Ebenso sind die Anforderungen für die Kommunikation mit dem SMGW vom BSI vorgeschrieben. Wer (neben dem Messstellenbetreiber) aus dem Internet direkt mit einem SMGW kommuniziert, wird als **externer Marktteilnehmer (EMT)** bezeichnet. Der EMT kommuniziert entweder mit dem SMGW, um Messwerte aus den modernen Messeinrichtungen zu empfangen, oder er nutzt das SMGW für die Kommunikation mit Geräten im Gebäude, die **Controllable Local Systems (CLS)** genannt werden. Das SMGW ist im letzteren Fall ein Proxy[1] und stellt lediglich den Kommunikationskanal bereit. Diese Kommunikation ist in Abbildung 2 dargestellt.

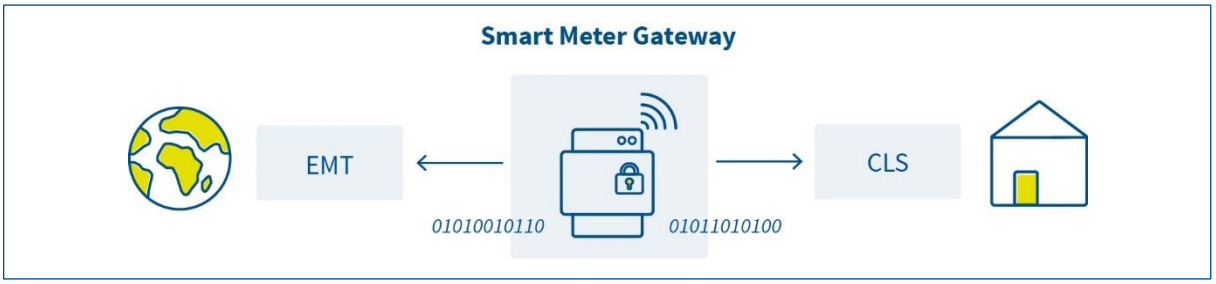

Abbildung 2 Kommunikation über SMGW

Das CLS könnte beispielsweise ein Gebäudeenergiemanagementsystem sein, das eine Ladestation oder eine Wärmepumpe steuert.

Per Definition ist ein EMT jede beliebige Instanz, die außer dem Gateway-Administrator (GWA) über das Internet mit einem SMGW kommunizieren darf. Die Rolle des GWA wird weiter unten genauer erläutert. Ein EMT muss also nicht zwingend ein Stromlieferant oder Netzbetreiber sein, sondern ist generisch definiert. Außerdem ist nicht vorgegeben, dass ein EMT überhaupt eine Funktion in der Energiewirtschaft haben muss. Es müssen jedoch unterschiedliche Auflagen erfüllt werden, damit eine Kommunikation möglich ist. Diese Auflagen werden in diesem Dokument zusammengefasst und eingeordnet.

Der Zweck der Kommunikation über SMGW ist regulatorisch offengehalten. Grundsätzlich ist es auch denkbar, dass Akteure außerhalb der Energiewirtschaft die Rolle des EMT wahrnehmen, beispielsweise im Bereich Smart Building oder Assisted Living. In diesen Fällen könnte die Internetverbindung des SMGW zum Beispiel für automatische Notrufe verwendet werden, unabhängig vom Internetanschluss der Kunden.

Auch wenn EMT nicht zwingend eine Rolle in der Energiewirtschaft haben müssen, wird in diesem Dokument der Fokus auf die Anwendung im Energiesystem gelegt. Alle darüber hinausgehenden Anwendungsfälle spielen bislang in der Praxis keine große Rolle.

1.2 Marktrollen im Energiesystem

Seit der Liberalisierung des Strommarktes in Deutschland und in der EU ist der Betrieb von Stromnetzen von der Energielieferung getrennt. Dementsprechend ist der **Netzbetreiber**, der das Netz betreibt, mit dem ein Kunde physikalisch verbunden ist, nicht mehr identisch mit dem **Lieferanten**, der die Energie am Markt oder mit eigenen Kraftwerken beschafft und an die Kunden verkauft. Als Netzbetreiber ist hier immer der Verteil-

[1] Ein Proxy ist ein Vermittler zwischen zwei Kommunikationsendpunkten. Client und Server kommunizieren dabei nicht direkt miteinander, sondern indirekt über den Proxy. In diesem Fall sind Client und Server die CLS-Einheit und der EMT, das SMGW ist der Proxy.

netzbetreiber als Anschlussnetzbetreiber gemeint. Neben der Trennung von Netzbetrieb und Energielieferung kann auch der Messstellenbetrieb, also der Ein- und Ausbau der Zähler sowie die Erfassung der Zählerdaten, vom Netzbetreiber an einen **Messstellenbetreiber (MSB)** übertragen werden. In diesem Fall kann es neben dem grundzuständigen MSB auch wettbewerbliche MSB geben, die unabhängig vom Netzbetreiber sind. Verbraucherinnen und Verbraucher können ihren MSB selbst wählen. MSB sind auch zuständig für den Einbau, die Konfiguration und den Betrieb von iMSys, also einschließlich der SMGW.

Die Akteure Netzbetreiber, Lieferanten und MSB nehmen im Energiesystem jeweils eine Marktrolle ein. Abbildung 3 zeigt vereinfacht die Energie- und Informationsflüsse zu den genannten Marktrollen. Hier ist zu betonen, dass das iMSys, bestehend aus moderner Messeinrichtung und SMGW, dem MSB gehört und von ihm eingebaut, konfiguriert und bei Bedarf ausgetauscht wird. Dementsprechend kommt dem MSB als Gateway-Administrator in der SMGW-Infrastruktur eine Schlüsselrolle zu.

In Abbildung 3 ist eine einfache Belieferung einer Kundin oder eines Kunden mit Energie unter Einbezug eines iMSys dargestellt, ohne Steuerungshandlungen, Einspeisung von Energie oder weitere Dienstleistungen. In dieser Darstellung übernimmt der MSB auch die Kommunikation von Messdaten mit dem SMGW, was heute üblich ist. Alternativ könnten Lieferant und Netzbetreiber jeweils direkt mit dem SMGW kommunizieren und müssten dann die Rolle des EMT einnehmen. Diese beiden Optionen werden in Kapitel 3.4 näher beleuchtet.

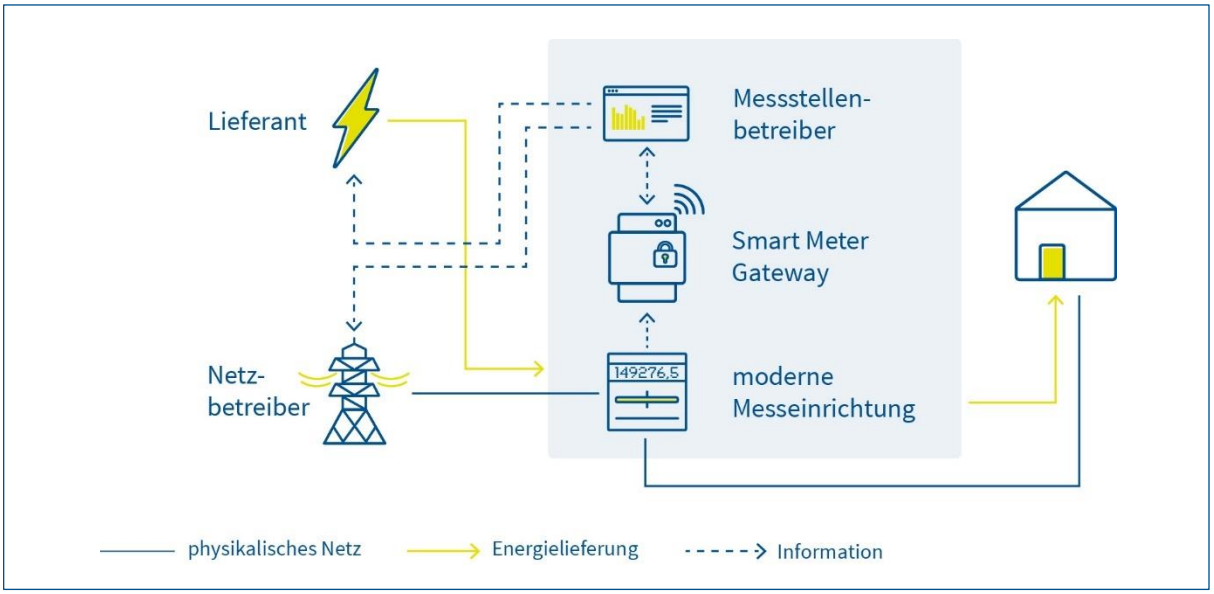

Abbildung 3 Darstellung der Marktrollen

2 Die Smart Metering Public Key Infrastruktur

Für die direkte Kommunikation mit dem SMGW muss von den Akteuren eine EMT-Rolle eingenommen werden. Eine wesentliche Voraussetzung für die Ausführung der EMT-Rolle ist die Teilnahme an der Smart Metering Public Key Infrastruktur (SM-PKI).

Eine Public Key Infrastruktur (PKI) ist ein im Internet sehr weit verbreitetes und bewährtes technisches Konzept, das es erlaubt, digitale Zertifikate auszustellen und zu verwenden. Es lässt sich mathematisch überprüfen, ob eine bestimmte (vertrauenswürdige) Instanz ein Zertifikat signiert hat oder nicht. Alle Teilnehmenden an dieser Infrastruktur besitzen dabei ein mathematisch verknüpftes Paar aus einem privaten und einem öffentlichen Schlüssel. Die Schlüssel sind letztlich lange Buchstaben- und Zahlenkombinationen. Wie die Namen bereits aussagen, kann der öffentliche Schlüssel veröffentlicht werden, während der private Schlüssel mit niemandem geteilt wird und im Extremfall nicht einmal aus einem speziellen Sicherheitsmodul auslesbar ist. Es ist für das Funktionieren jeder PKI essenziell, dass private Schlüssel niemals weitergegeben werden.

Da es nahezu unmöglich ist, aus dem öffentlichen Schlüssel den privaten Schlüssel zu berechnen, zählt die Kenntnis über den privaten Schlüssel als Identitätsnachweis. Es lässt sich über Verschlüsselungs- und Entschlüsselungsalgorithmen nachweisen, dass man zu dem eigenen öffentlichen Schlüssel auch den privaten Schlüssel besitzt. Wird eine Information mit dem öffentlichen Schlüssel verschlüsselt, kann sie nur mit dem privaten Schlüssel entschlüsselt werden, also nur von einer einzigen Instanz. Wird eine bekannte Information mit dem privaten Schlüssel verschlüsselt, kann sie von jedem mit dem öffentlichen Schlüssel entschlüsselt werden. Unter Kenntnis der ursprünglichen unverschlüsselten Information ist damit der Nachweis erbracht, dass die Information vom Besitzer des privaten Schlüssels verschlüsselt worden sein muss. Damit kann Identität nachgewiesen werden (Wendzel, 2018).

Zudem ist es auch möglich, mithilfe des eigenen privaten Schlüssels Zertifikate auszustellen. Über den öffentlichen Schlüssel können alle überprüfen, ob der private Schlüssel für die Ausstellung des Zertifikats benutzt wurde, und damit feststellen, ob das Zertifikat von einer bestimmten vertrauenswürdigen Instanz kommt oder nicht. Diese vertrauenswürdigen Instanzen werden **Certificate Authorities (CA)** genannt. Eine CA kann von einer weiteren CA zertifiziert werden und diese von einer weiteren usw., wodurch sich ein Baum von Zertifizierungsbehörden aufspannen lässt. Letztlich funktioniert eine PKI allerdings nur, wenn alle Teilnehmenden einem gemeinsamen Vertrauensanker vertrauen, der **Root-CA**, die ebenfalls einen öffentlichen und einen privaten Schlüssel besitzt und **Sub-CAs** zertifizieren kann. Im Falle der SM-PKI ist diese Root-CA in Besitz des BSI (Bundesamt für Sicherheit in der Informationstechnik, 2023c).

2.1 Systemarchitektur der SM-PKI

Die Systemarchitektur der SM-PKI wird in der Technischen Richtlinie TR-03109-4 des BSI (Bundesamt für Sicherheit in der Informationstechnik, 2017) festgelegt. Den hoheitlichen Vertrauensanker bildet die Root-CA beim BSI. Von ihr werden die Sub-CAs zertifiziert, die in einem Unternehmen – beispielsweise einem Messstellenbetreiber – oder unternehmensübergreifend betrieben werden und letztlich die Endnutzer zertifizieren. Zu den Endnutzern gehören EMT, SMGW, GWA und Gateway-Hersteller (GWH) und damit einzelne Geräte oder Marktteilnehmer. Die Struktur ist in Abbildung 4 dargestellt.

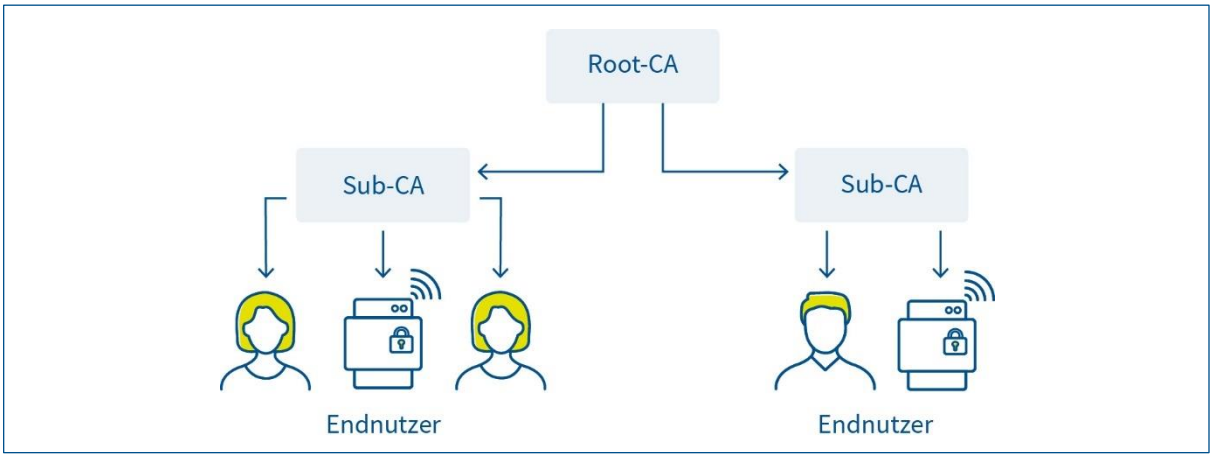

Abbildung 4 Die Architektur der SM-PKI

2.2 Rollen und Aufgabengebiete in der SM-PKI

Im Folgenden werden die jeweiligen Rollen und Aufgabengebiete in der SM-PKI beschrieben. Dies sind die Zertifizierungsstellen Root-CA und die Sub-CAs sowie die Endnutzer, worunter EMT, GWA, GWH und SMGW fallen.

2.2.1 Root-CA

Die Root-CA bildet den zentralen Vertrauensanker der SM-PKI und ist beim BSI verortet. Von ihr werden sämtliche Sub-CAs registriert und zertifiziert. EMT müssen mit der Root-CA in keinem direkten Kontakt stehen, sondern nur mit der entsprechenden Sub-CA.

2.2.2 Sub-CA

Jede Sub-CA übernimmt die Registrierung und Zertifizierung der Endnutzer, darunter auch EMT. Darüber hinaus kümmert sich die Sub-CA um den operativen Betrieb der Zertifikate für EMT, darunter der Zertifikatswechsel und die Veröffentlichung von Sperrlisten. Wer als EMT an der SM-PKI teilnehmen möchte, muss (direkt oder über einen Dienstleister) Kontakt zu einer Sub-CA aufnehmen. Mehr dazu in Kapitel 2.3.

2.2.3 Endnutzer

Jeder Endnutzer der SM-PKI wird von einer Sub-CA zertifiziert und erhält dadurch die notwendigen Zertifikate für die authentizitätsgesicherte und verschlüsselte Kommunikation mit anderen Endnutzern. Es gibt vier Kategorien von Endnutzern:

- Externer Marktteilnehmer (EMT)
- Gateway-Administrator (GWA)
- Gateway-Hersteller (GWH)
- Smart Meter Gateway (SMGW)

Ein EMT ist jede beliebige Instanz, die außer dem GWA über das Internet mit dem SMGW kommunizieren darf. Neben Stromlieferanten und Netzbetreibern können also auch andere Akteure die Rolle übernehmen. Die Rolle des **EMT** wird in diesem Bericht in Kapitel 3 ausführlich beschrieben.

Der **GWA** hat die Aufgabe der Administration der ihm zugeordneten SMGW. Er ist die einzige Instanz, die das SMGW konfigurieren kann (Bundesamt für Sicherheit in der Informationstechnik, 2021). Dementsprechend müssen EMT bei dem jeweiligen GWA die entsprechende Konfiguration der SMGW bestellen, damit eine Kommunikation mit den SMGW überhaupt möglich ist. Darüber hinaus ist es ausschließlich dem GWA erlaubt, den CLS-Kanal aus dem Internet zu initialisieren. Falls der EMT die Verbindung über den CLS-Kanal initialisieren möchte, zum Beispiel im Rahmen einer Steuerungshandlung, und die Verbindung nicht durch das SMGW oder durch die CLS-Einheit hergestellt wird, muss er den Weg ebenfalls über den GWA gehen. Andernfalls ist der Verbindungsaufbau nur „von innen nach außen“ möglich, also von der CLS-Einheit oder vom SMGW, beispielsweise in regelmäßigen Zeitintervallen oder basierend auf bestimmten gemessenen Ereignissen. Auch diese Option muss zunächst durch den GWA durch die entsprechende Konfiguration mit sogenannten HAN-Kommunikationsszenarien (HKS) ermöglicht werden, die in Tabelle 1 zusammengefasst sind.

HAN-Kommunikations-szenario (HKS)	Verbindungsaufbau
HKS 3	Die CLS-Einheit initiiert die Verbindung mit dem SMGW, dieses initiiert dann die Verbindung mit dem EMT.
HKS 4	Der GWA initiiert die Verbindung mit dem SMGW (ggf. auf Anfrage des EMT), das SMGW initiiert anschließend die Verbindung mit CLS und EMT.
HKS 5	Das SMGW initiiert die Verbindung mit CLS und EMT, z. B. in regelmäßigen Zeitintervallen oder aufgrund einer bestimmten Messung.

Tabelle 1 HAN-Kommunikationsszenarien

Dementsprechend kommt dem GWA eine zentrale Rolle auch für EMT zu. Der GWA ist entweder der MSB oder ein Dienstleister des MSB und für den technischen Betrieb des SMGW verantwortlich (vgl. § 2 Abs. 20 MsbG). Auch wenn manche Hersteller und Betreiber von GWA-Software gleichzeitig registrierte Betreiber einer Sub-CA sind, ist die Rolle des GWA nicht zwingend mit der einer Sub-CA identisch.

GWH produzieren SMGW und bringen ihnen im Herstellungsprozess Gütesiegelzertifikate auf. GWH sind zwar auch Endnutzer der SM-PKI, spielen jedoch für die operative Kommunikation über SMGW keine Rolle.

Das **SMGW** ist als einziger Endnutzer der SM-PKI weder eine natürliche noch eine juristische Person. Es wird daher nur technisch wie ein Endnutzer behandelt. Organisatorisch werden alle Aufgaben in der SM-PKI (z. B. das Beantragen von Zertifikaten) durch den GWA wahrgenommen.

2.3 Teilnahme an der SM-PKI

Damit Endnutzer an der SM-PKI teilnehmen können, benötigen sie Zertifikate, die von einer Sub-CA ausgestellt wurden. Dabei handelt es sich um drei Zertifikate, die für drei unterschiedliche Zwecke (Transport Layer Security (TLS), Verschlüsselung und Signatur) eingesetzt werden. Sie haben eine Laufzeit von maximal zwei Jahren und müssen daher regelmäßig erneuert werden. Im Folgenden wird der Fokus auf EMT als Endnutzer in der SM-PKI gelegt.

Um die Zertifikate zu bekommen und an der SM-PKI teilnehmen zu können, muss sich ein EMT bei einer Sub-CA registrieren. Für diesen Zweck gibt es für jede Sub-CA eine Registrierungsstelle (Registration Authority,

RA). Dort werden Antragsteller identifiziert und authentifiziert (Bundesamt für Sicherheit in der Informationstechnik, 2023a, Kap. 1.3.2). Einen Überblick über alle registrierten Sub-CAs stellt das BSI auf seiner Website[2] bereit. Jede Sub-CA muss auf ihrem Webauftritt unter anderem ihre Kontaktdaten, die aktuellen Zertifikate und ihre jeweilige Certificate Policy veröffentlichen (Bundesamt für Sicherheit in der Informationstechnik, 2023a, Kap. 2.2.2).

Übersicht über registrierte Sub-CAs

Um sich als EMT zu registrieren, ist die Kontaktaufnahme zu einer Sub-CA erforderlich. Eine Übersicht über alle registrierten Sub-CAs ist auf der Website des BSI zu finden.

Die beim BSI aufgeführten Zertifizierungsstellen müssen auf ihrer Website über ihre Certificate Policy informieren, was bedeutet, dass die konkreten Anforderungen für die Registrierung und Identifizierung öffentlich eingesehen werden können. Dazu gehört beispielsweise der Prozess für den Identitätsnachweis des Antragstellers. In jedem Fall sind für die Registrierung als EMT

- Name und Anschrift der Organisation,
- Organisationsnachweis (z. B. Auszug aus dem Handelsregister) und
- Kontaktdaten der Ansprechpartner und vertretungsberechtigten Personen

notwendig (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 3.2.2.2). Außerdem müssen eine Erklärung für die Verwendung der Zertifikate sowie ein Nachweis der Sicherheitsanforderungen (mehr dazu in Kapitel 4.1) vorliegen. Für die Kommunikation mit der Sub-CA sind außerdem persönliche E-Mail-Zertifikate notwendig. Vor dem Wirkbetrieb müssen die Prozesse zum Zertifikatsmanagement (Erneuerung, Sperrung etc.) mit Test-Zertifikaten getestet werden.

Wenn die Sub-CA erfolgreiche Tests bestätigt, wird das EMT-Zertifikat durch die Sub-CA ausgestellt.

Es ist zulässig, sowohl die Kommunikation mit den SMGW als auch das Zertifikatsmanagement an einen Dienstleister auszulagern. Dabei ist jedoch darauf zu achten, dass die Kommunikation zwischen Auftraggeber und Dienstleister den kryptografischen Anforderungen für iMSys genügt (Bundesamt für Sicherheit in der Informationstechnik, 2022). Diese Option wird näher in Kapitel 4.3 beschrieben.

[2] https://www.bsi.bund.de/dok/smgw-registrierte-sub-cas

3 Externe Marktteilnehmer und Energieservice-anbieter

Organisationen, die Messdaten aus iMSys empfangen und verarbeiten möchten, haben die Wahl zwischen zwei Rollen, die ihnen den Datenempfang ermöglichen:

Externe Marktteilnehmer (EMT) sind dadurch definiert, dass sie aus dem Internet (WAN) direkt mit SMGW kommunizieren können. Sie sind Endnutzer der SM-PKI und müssen alle entsprechenden Anforderungen erfüllen. Dem BSI zufolge kann entweder eine gesamte Organisation oder nur ein von der Organisation verwendetes Kommunikationssystem als EMT bezeichnet werden.

Energieserviceanbieter (ESA) können im Auftrag der Anschlussnutzer Daten beim Messstellenbetreiber bestellen (Bundesnetzagentur, 2022c). Bei diesen Daten kann es sich um historische Daten oder Live-Daten handeln. Die Daten können auch vom Backend des MSB empfangen werden. ESA kommunizieren nicht zwingend direkt mit SMGW und müssen dementsprechend nicht zwingend an der SM-PKI teilnehmen. Es ist davon auszugehen, dass Marktteilnehmer, die Messdaten aus iMSys verarbeiten wollen, aufgrund der niedrigeren Anforderungen eher die Rolle des ESA einnehmen als die des EMT. Die Rolle des ESA wird in Kapitel 3.2 näher beschrieben.

Im Folgenden werden diese Rollen genauer dargestellt und es wird der Unterschied zwischen aktiven EMT (aEMT) und passiven EMT (pEMT) deutlich gemacht.

3.1 Die unterschiedlichen EMT-Rollen

Grundsätzlich gibt es zwei EMT-Rollen: aktive externe Marktteilnehmer (aEMT) und passive externe Marktteilnehmer (pEMT). Da pEMT nur Daten empfangen und den CLS-Kanal nicht nutzen und damit nicht steuern, müssen sie niedrigere Anforderungen erfüllen als aEMT (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 1.3.3.4).

3.1.1 Aktiver EMT (aEMT)

Ein aEMT ist dadurch charakterisiert, dass er über das SMGW mit CLS-Einheiten kommunizieren kann. Aktive EMT können das SMGW als Kommunikations-Gateway für unterschiedlichste Anwendungsfälle verwenden. Aktive EMT können beispielsweise Verteilnetzbetreiber sein, die im Zuge eines Netzengpasses eine steuerbare Verbrauchseinheit dimmen. Die Rolle des aEMT ist nicht auf energiewirtschaftliche Anwendungsfälle beschränkt und kann auf andere Dienste erweitert werden, für die ein sicherer und standardisierter Kommunikationskanal zum Gebäude einen Mehrwert bringt. Da ein aEMT auch alle Anforderungen erfüllen muss, die für pEMT gelten, schließt die Rolle des aEMT die des pEMT mit ein.

3.1.2 Passiver EMT (pEMT)

Ein pEMT kann keine CLS-Einheiten ansprechen, sondern lediglich Daten von SMGW empfangen und mit anderen Teilnehmenden der SM-PKI Daten austauschen. Es ist für pEMT nicht möglich, einen Kommunikationskanal über das SMGW zum Letztverbraucher aufzubauen.

Passive EMT können beispielsweise Stromlieferanten sein, die Verbrauchsdaten in der zeitlichen Auflösung erhalten, die für die jeweiligen Tarife notwendig ist, zum Beispiel viertelstündlich. Eine Steuerung findet nicht statt. Zu beachten ist zudem, dass lediglich das Empfangen von Messdaten aus dem iMSys in der Rolle des pEMT möglich ist, also etwa Daten von Strom-, Wasser-, Gas- oder Wärmezählern. Jede weitere Kommunikation aus dem Heimnetz über SMGW erfordert die Rolle des aEMT, selbst wenn dabei nur Daten aus dem Heimnetz empfangen werden und keine Steuerung vorgenommen wird. Dazu gehören zum Beispiel Daten von Messgeräten, die zusätzlich zu den eichrechtskonformen modernen Messeinrichtungen verbaut wurden und nicht über das entsprechende Zähler-Netzwerk (LMN) mit dem SMGW verbunden sind. Hierzu zählt beispielsweise ein Messgerät an der Batterie, das deren aktuelle Lade- und Entladeleistung misst und die Daten an das Backend des Energiemanagementdienstleisters sendet. Soll hierfür die SMGW-Infrastruktur verwendet werden, muss das Backend die Rolle des aEMT einnehmen.

3.2 Energieserviceanbieter (ESA)

Die Rolle des Energieserviceanbieters (ESA) ist eine von der Bundesnetzagentur nachträglich eingeführte Marktrolle. Sie wurde etabliert, um eine standardisierte Bereitstellung von Messdaten an Energiedienstleister und Energiedatenmanager zu vereinfachen (Bundesnetzagentur, 2020). Ein ESA kann im Auftrag des Anschlussnutzers Werte beim MSB anfragen und sie verarbeiten. Da im Sinne der Marktkommunikation (MaKo) 2022 (beschrieben in Kapitel 3.4.3) die Messwerte ohnehin vom SMGW an den MSB geschickt und von dort verteilt werden dürfen, können – mit der entsprechenden rechtlichen Grundlage – auch von dort die Messwerte empfangen werden. ESA können diese Messdaten in unterschiedlicher Auflösung für verschiedene Zeiträume empfangen und auswerten. Ein Anwendungsfall kann beispielsweise der Einsatz in Planungsbüros sein, die Messwerte des historischen Stromverbrauchs eines Gebäudes anfordern, um neue Photovoltaikanlagen oder Ladestationen am Gebäude zu dimensionieren. Ein anderes Beispiel sind Dienstleister, die den Stromverbrauch visualisieren und analysieren und auf dieser Basis Stromspartipps anzeigen können. Es ist auch möglich, als ESA turnusmäßig Daten zu empfangen. Die Daten kommen entweder vom SMGW selbst oder vom Backend des MSB. Um Daten direkt vom SMGW zu empfangen, muss der ESA die Rolle des EMT einnehmen, um die Daten vom Backend des MSB zu empfangen jedoch nicht. In beiden Fällen werden die Daten im XML-Format (Extensible Markup Language) versendet. Im Falle des Versands aus dem Backend des MSB ist das Format EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) vorgesehen.

Für den Empfang von Messwerten aus dem Backend des MSB sind lediglich die Regelungen zum Übertragungsweg des Bundesverbands der deutschen Energie- und Wasserwirtschaft (BDEW) (BDEW, 2021) zu beachten, nicht jedoch die BSI-Anforderungen aus der SM-PKI. Die Übermittlung der Werte an den ESA darf allerdings keinen Bezug zur Netznutzungs-, Bilanzkreis- oder Mehr-/Mindermengenabrechnung haben (Bundesnetzagentur, 2022c).

3.3 Potenzielle Marktteilnehmer

Die technischen Richtlinien des BSI machen keine Vorgaben hinsichtlich der Marktrollen oder Branchen, die auf EMT zutreffen müssen. Es ist demnach auch nicht vorgegeben, dass EMT in der Energiewirtschaft tätig sind. Daher sind die Möglichkeiten der potenziellen Marktteilnehmer sehr groß. Dennoch sollen in Tabelle 2 zur Veranschaulichung einige Beispiele für die Rollen von EMT und ESA dargestellt werden.

Marktteilnehmer	EMT/ESA-Rolle	Begründung
Ein Lieferant möchte dynamische Tarife anbieten und muss sie dementsprechend stundenscharf abrechnen.	pEMT	Eine Steuerung ist nicht notwendig. Da die Abrechnung einen Bezug zur Mehr-/Mindermengenabrechnung bzw. Bilanzkreisabrechnung hat, scheidet die Rolle des ESA aus.
Ein Aggregator steuert Batterien über iMSys und verkauft die Flexibilität am Regelenergiemarkt.	aEMT	Eine Steuerung über iMSys ist nur für aEMT möglich.
Ein Planungsbüro dimensioniert Photovoltaikanlagen und möchte daher den bisherigen Energiebedarf auswerten.	ESA	Die Daten sind am einfachsten als ESA zu beziehen.
Ein Verteilnetzbetreiber muss steuerbare Verbrauchseinrichtungen im Falle von Netzengpässen abregeln.	aEMT	Die Steuerung ist nur für aEMT möglich.
Ein Pflegedienst wird automatisch informiert, wenn Sensoren in der Wohnung einen Sturz registrieren. Eine Internetverbindung der Kunden existiert nicht.	aEMT	Das Empfangen der Sensordaten, die nicht von einer modernen Messeinrichtung erfasst werden, erfordert die Verwendung des CLS-Kanals, der nur für aEMT zur Verfügung steht.
Ein Dienstleister möchte über ein Webinterface Stromspartipps basierend auf dem aktuellen Verbrauch anbieten.	ESA	Die Daten sind am einfachsten als ESA zu beziehen.

Tabelle 2 Beispiele für potenzielle Marktteilnehmer

3.4 Marktkommunikation (MaKo)

Die MaKo beschreibt die Kommunikation zwischen Organisationen in der Energiewirtschaft und geht deutlich über die SMGW-Infrastruktur hinaus. Zur MaKo gehören unter anderem Abrechnungen von Energiemengen, Informationen über Lieferantenwechsel von Kunden und Redispatch, also Fahrplananpassungen aufgrund von Netzengpässen. Eine definierte MaKo ist erforderlich, damit die unterschiedlichen Akteure (Lieferanten, Netzbetreiber, Messstellenbetreiber) im liberalisierten Strommarkt standardisiert und effizient Daten austauschen können. Mit dem Rollout von iMSys musste auch eine Möglichkeit geschaffen werden, wie iMSys mit Akteuren am Energiemarkt kommunizieren.

3.4.1 Zielmodell

Das im Messstellenbetriebsgesetz (MsbG) beschriebene und in Abbildung 5 gezeigte Zielmodell sieht vor, dass alle relevanten Daten aus dem iMSys direkt an die Empfänger gesendet werden. Die Empfänger müssen demnach alle die Rolle eines EMT einnehmen und für jeden Empfänger muss durch den Gateway-Administrator eine neue Verbindung konfiguriert werden.

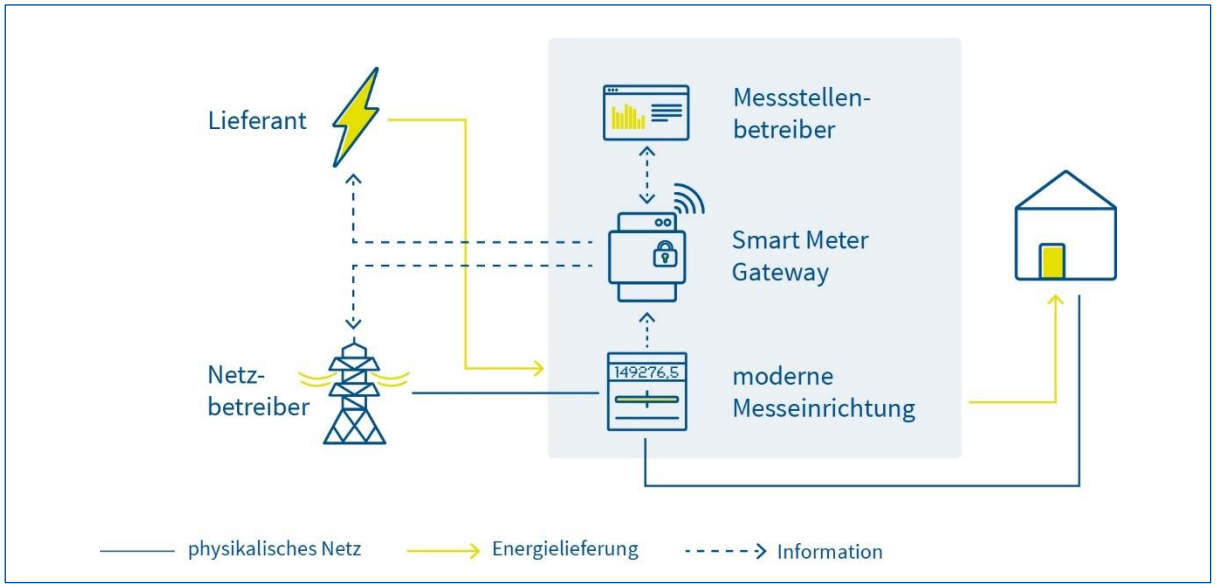

Abbildung 5 Zielmodell der Marktkommunikation (MaKo)

3.4.2 Interimsmodell MaKo 2020

Da das Zielmodell durch die SMGW der ersten Generation zunächst nicht durchführbar war, wurde mit der MaKo 2020 von der Bundesnetzagentur ein Interimsmodell eingeführt, das in Abbildung 6 dargestellt ist. Es sieht vor, dass alle Messdaten zunächst an den GWA geschickt und von dort sternförmig weiterverteilt werden. Die Informationsflüsse sind vergleichbar mit dem analogen Messstellenbetrieb ohne SMGW, in dem Beschäftigte des MSB vor Ort die Zähler ablesen und der MSB die Messwerte dann weitergibt. In diesem Fall müssen weder Netzbetreiber noch Lieferanten die Rolle des EMT einnehmen, da sie nicht mit dem SMGW kommunizieren. Für sie gelten jedoch auch unabhängig davon regulatorische Vorgaben zur IT-Sicherheit.

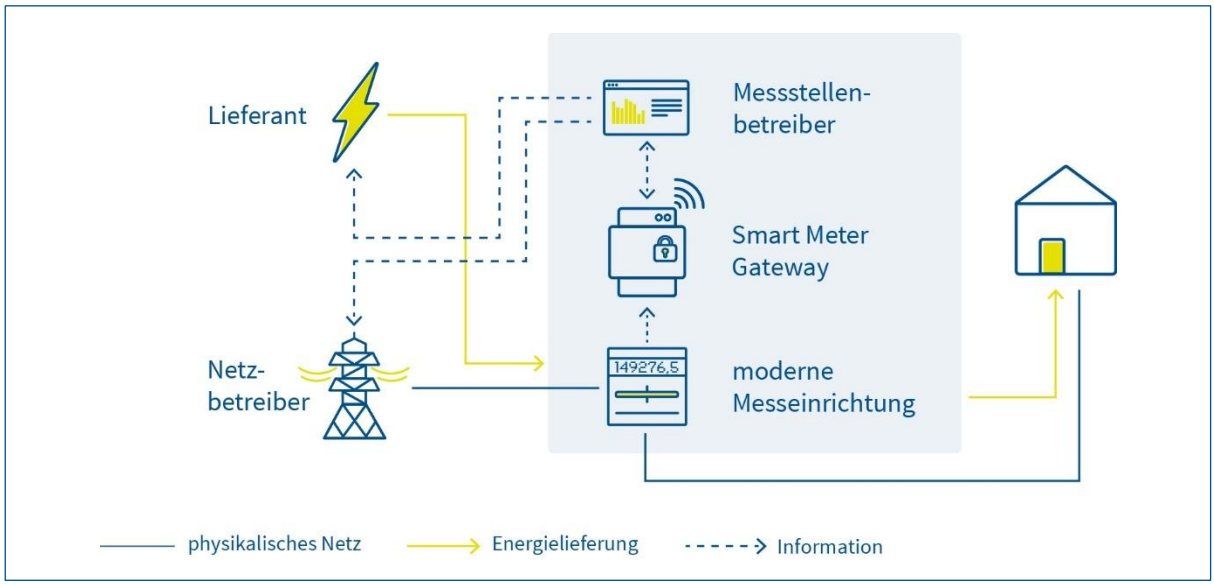

Abbildung 6 Interimsmodell Mako 2020

3.4.3 MaKo 2022 und Universalbestellprozess

Die aktuellen Festlegungen zum Datenaustausch mit iMSys der Bundesnetzagentur sind in der MaKo 2022 zusammengefasst. Sie wurden im Jahr 2020 beschlossen und sind seit dem Jahr 2022 gültig (Bundesnetzagentur, 2020). Die MaKo geht wie oben bereits erwähnt deutlich über die Kommunikation mit iMSys hinaus und wird daher hier nur in Teilen erklärt. Sie umfasst folgende Prozesse:

- **Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE)**, was hauptsächlich Prozesse für den Wechsel des Stromlieferanten betrifft
- **Wechselprozesse im Messwesen (WiM)**, wodurch Änderungen im Messbetrieb (insbesondere iMSys) in verschiedenen Anwendungsfällen beschrieben werden. Dazu gehören auch der erstmalige Einbau eines iMSys und die entsprechende Konfiguration für EMT.
- **Marktprozesse für erzeugende Marktlokationen (MPES)** wie Photovoltaikanlagen
- **Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom (MaBiS)**, was eine sehr umfangreiche Beschreibung zur Koordination und Kommunikation von Bilanzkreisen darstellt und nur für Akteure relevant ist, die Bilanzkreise bewirtschaften und Informationen darüber austauschen bzw. koordinieren, also in erster Linie Lieferanten und Netzbetreiber

Ferner gehören zur MaKo 2022 folgende Dokumente:

- Eine (verpflichtend anzuwendende) Vorlage für den **Netznutzungsvertrag** zwischen Netzbetreiber und Lieferanten bzw. Letztverbrauchern,
- Vorgaben für den **Elektronischen Datenaustausch (EDI)** in allgemeiner Form, wobei die bereits erwähnten „Regelungen zum Übertragungsweg“ des BDEW (BDEW, 2021) referenziert werden, sowie
- **Netzzugangsregeln zur Ermöglichung einer ladevorgangsscharfen bilanziellen Energiemengenzuordnung für Elektromobilität (NZR-EMob)**, wodurch bestimmte Regeln zwischen Ladestationsbetreibern (Charge Point Operator, CPO) und den Netzbetreibern, die die entsprechenden Ladestationen anschließen, definiert werden.

Hier wird deutlich, dass die meisten Festlegungen nicht direkt die regulatorischen Vorgaben für EMT betreffen und hier deshalb nur der Vollständigkeit halber aufgeführt sind. Hauptsächlich relevant sind die

Wechselprozesse im Messwesen (WiM) und die Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE). Diese beiden Dokumente wurden Ende 2022 erneut geändert. Mit dieser Änderung wurde der **Universalbestellprozess** eingeführt (Bundesnetzagentur, 2022a). Er legt unter anderem die Abwicklung von Steuerungshandlungen in Verbindung mit iMSys sowie die Bestellung von Konfigurationen des iMSys beim MSB fest.

Wesentliche Änderungen durch den Universalbestellprozess sind folgende (Bundesnetzagentur, 2022b) (Bundesnetzagentur, 2022c):

- Die Einführung einer **Netzlokation**, um einen „digitalen Netzanschluss“ zu ermöglichen
- Die Einführung von Schaltzeitdefinitionen, Steuererlaubnissen und Leistungskurvendefinitionen. In Kapitel 5 der GPKE werden Steuerbefehle vom Lieferanten oder Netzbetreiber an einen MSB definiert. Schaltbefehle (z. B. nach § 14a EnWG) werden standardisiert an den MSB übermittelt, der sie an das iMSys weiterleitet.
- Die Festlegung, dass der Datenaustausch zwischen Marktpartnern über **API-Webdienste** nach den Vorgaben der EDI@Energy erfolgen muss
- Eine Unterscheidung von Werten nach **Typ 1** und **Typ 2**. Erstere betreffen Werte, die für die Netznutzungs-, Bilanzkreis- oder Mehr-/Mindermengenabrechnung verwendet werden und sind für die Rolle des ESA ausgeschlossen. Alle anderen Werte (Typ 2) können vom ESA empfangen und verarbeitet werden.

Grundsätzlich sind im Universalbestellprozess sowohl die sternförmige Kommunikation aus dem iMSys als auch der Versand von Messwerten aus dem Backend des MSB vorgesehen.

Für die (potenziellen) Nutzer der SMGW-Infrastruktur in der Rolle des EMT oder ESA bedeutet der Universalbestellprozess Folgendes:

1. Konfigurationen von SMGW sowie der Einbau von iMSys sind beim MSB standardisiert bestellbar.
2. Schaltzeitendefinitionen, Zählzeitdefinitionen und Leistungskurvendefinitionen können von Lieferanten und Netzbetreibern beim MSB bestellt werden.
3. Der Empfang von Messdaten ist aus dem Backend des MSB oder direkt aus dem iMSys möglich.

4 Regulatorische Voraussetzungen

Damit eine Organisation als externer Marktteilnehmer die SMGW-Infrastruktur nutzen darf, muss sie unterschiedliche regulatorische Anforderungen erfüllen. Diese sind auf verschiedenen Ebenen definiert:

An oberster Stelle stehen die **Gesetze**. Für den Fall der SMGW-Infrastruktur ist das *Messstellenbetriebsgesetz* (MsbG) am relevantesten. Das MsbG definiert zwar einige Pflichten für Gateway-Administratoren und -Hersteller sowie für den Betrieb und die Nutzung der SMGW-Infrastruktur, macht jedoch keine detaillierten Vorgaben für die Rolle des EMT. Stattdessen wird definiert, dass die diesbezüglichen Vorgaben des BSI einzuhalten sind. Darüber hinaus definiert das *Energiewirtschaftsgesetz* (EnWG) die wesentlichen gesetzlichen Vorgaben für Prozesse in der Energiewirtschaft.

Sofern es die Gesetze über Verordnungsermächtigungen erlauben, kann die Bundesregierung, meistens das *Bundesministerium für Wirtschaft und Klimaschutz (BMWK)*, **Verordnungen** erlassen, die in der Regel diese Gesetze konkretisieren. Hierzu zählt beispielsweise die Klarstellung, welche Mess- und Steuerungsvorgänge energiewirtschaftlich relevant sind und ausschließlich über SMGW erfolgen dürfen (vgl. § 19 MsbG). Demnach müssen alle Akteure, die solche Steuerungsvorgänge durchführen, die Rolle des EMT einnehmen oder einen Dienstleister dafür beauftragen.

Die für EMT relevanten **behördlichen Vorgaben** werden vom BSI und von der Bundesnetzagentur formuliert. Die wichtigsten Vorgaben des BSI sind hier die *Technischen Vorgaben für intelligente Messsysteme und deren sicherer Betrieb BSI TR-03109*. Hier werden die Rolle des EMT sowie seine organisatorischen und technischen Anforderungen definiert. Die Bundesnetzagentur definiert mit ihren Vorgaben zur *Marktkommunikation* Regeln für die Kommunikation in der Energiewirtschaft, die über die Kommunikation in der SMGW-Infrastruktur hinausgehen.

Während Gesetze und behördliche Vorgaben rechtlich bindend sind, gibt es **Normen und Standards** aus Branchengremien, die grundsätzlich nicht zwingend eingehalten werden müssen. Jedoch werden sie an manchen Stellen von Behörden referenziert, wodurch ihnen ebenfalls ein regulativer Charakter zukommt. Die Rolle des EMT betrifft hier die *ISO/IEC 270001*, die vom BSI referenziert wird und einen internationalen Standard für ein Informationssicherheits-Managementsystem darstellt. Für energiewirtschaftliche Akteure, die typischerweise als EMT infrage kommen, sind außerdem die Datenformate *EDI@Energy* des BDEW sowie Hinweise und Anwendungsregeln des VDE-FNN relevant, die von der Bundesnetzagentur referenziert werden.

Abbildung 7 Hierarchie der regulatorischen Vorgaben

Im Folgenden werden die Anforderungen zusammengefasst, die speziell für die Rolle des EMT definiert sind. Sie werden hauptsächlich durch die oben genannten BSI-Richtlinien vorgegeben. Für Organisationen, denen die Erfüllung der nachfolgenden Anforderungen zu aufwendig erscheint, kann die Inanspruchnahme eines Dienstleisters eine attraktive Option darstellen. Sie wird in Kapitel 4.3 näher beschrieben.

4.1 Voraussetzungen und Anforderungen an EMT

Die Certificate Policy der SM-PKI (Bundesamt für Sicherheit in der Informationstechnik, 2023b) als Teil der BSI TR-03109 definiert Voraussetzungen und Anforderungen, die EMT erfüllen müssen. Sie unterscheiden sich je nach EMT-Rolle (pEMT oder aEMT) und variieren hinsichtlich Komplexität, Zeitaufwand und anfallender Kosten. Grundsätzlich gibt es **organisatorische, betriebliche, physikalische und technische Sicherheitsanforderungen**. Einige organisatorische, betriebliche und physikalische Anforderungen gelten allerdings für alle EMT. Dies sind folgende (wörtlich aus der Certificate Policy (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 5.2) übernommen):

- **Objektschutz:** Die betrieblichen Prozesse müssen vor Störung geschützt werden.
- **Zutrittssicherheit:** Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getroffen werden.
- **Informationsträger:** Bei der Verarbeitung und Aufbewahrung von Informationen in IT-Systemen MUSS der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch gewährleistet werden. Wenn nicht mehr benötigt, MUSS der Informationsträger sicher und unwiederherstellbar zerstört werden. […]
- **Einhaltung von Verpflichtungen:** Basierend auf den verschiedenen Aufgaben MÜSSEN die Mitarbeiter die Pflichten entsprechend ihren Rollen bei ihren Tätigkeiten einhalten.
- **Beschränkung der Anzahl Mitarbeiter:** Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, MUSS auf die unbedingt notwendige Anzahl begrenzt sein.
- **Eskalationsmanagement:** Es MUSS ein gut definiertes und eindeutiges Eskalationsmanagement umgesetzt werden. […]
- **Rollen und Verantwortungen:** Die Rollen und Verantwortlichkeiten sind gemäß den Anforderungen in Kapitel 5.2.2 [der BSI Certificate Policy der SM-PKI] zu dokumentieren. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus MÜSSEN die Verantwortlichkeiten klar definiert werden.
- **Rollenbeschreibungen:** Für temporäres und permanentes Personal MÜSSEN Rollenbeschreibungen definiert werden, welche Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten.
- **Einhaltung der ISMS-Anforderungen:** Das Personal MUSS administrative und betriebliche Verfahren und Prozesse im Einklang mit dem ISMS bzw. dem Sicherheitskonzept (passiver EMT) durchführen. […]
- **Archivierung der öffentlichen Schlüssel:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.
- **Definition der zu archivierenden Informationen:** Die Informationen, welche für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, MÜSSEN klar definiert werden.

- **Kryptografiemodule:** Die Schlüssel MÜSSEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden. […]
- **Schutz der Speichermedien:** Die Speichermedien MÜSSEN gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z. B. Feuer) gesichert werden […].
- **Schlüsselaufbewahrung:** Die Speichermedien MÜSSEN sich in einem physisch und logisch hoch gesicherten Bereich befinden. Der Zutritt MUSS auf eine klar definierte Anzahl von Personen eingeschränkt werden.
- **Vertrauenswürdiges Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdiges Personal erzeugt und gespeichert werden.
- **Abfallbeseitigung:** Es MUSS sichergestellt werden, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen veröffentlicht werden können.
- **Gehärtete IT-Systeme:** Es MUSS sichergestellt werden, dass die Anforderungen an gehärtete IT-Systeme und -Netzwerke sowie an die physische Sicherheit eingehalten werden. Eine Basis für umzusetzende Maßnahmen kann aus dem BSI-Grundschutzkatalog entnommen werden.
- Bei einer **Kompromittierung** oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels MUSS das zugehörige Zertifikat unverzüglich gesperrt und DARF NICHT wiederverwendet werden. […]
- Ein Fall von Kompromittierung sowie Verdachtsfälle MÜSSEN durch den Schlüsselinhaber dokumentiert werden.
- Jeder begründete Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels ist aufzuklären.
- Die **Generierung neuer Schlüssel und Zertifikate** MUSS überwacht und dokumentiert werden. […]
- **Notfallmanagement:** […] EMT MÜSSEN angemessen auf Störungen oder Notfälle reagieren, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten.
- **Kompromittierung:** Wenn die Vermutung besteht, dass Schlüsselmaterial kompromittiert ist, so DARF KEIN PKI-Teilnehmer dieses weiter nutzen.
- **Risikoreduktion / Schadensminderung:** Alle PKI-Teilnehmer SOLLTEN entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden.
- **Vermeidung von Vorfällen:** Alle PKI-Teilnehmer MÜSSEN angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden.
- **Vorgehen nach einer Störung:** Nach einer schweren Störung MÜSSEN alle PKI-Teilnehmer sicherstellen, dass die entstandene Sicherheitslücke geschlossen wird.

Darüber hinaus müssen die Zertifikatsbeantragung sowie das Incident- oder Notfall-Management bezüglich zertifikatsrelevanter Vorfälle archiviert werden. Die Kompromittierung des privaten Schlüssels oder andere sicherheitsrelevante Vorfälle müssen an die Sub-CA gemeldet werden. Außerdem muss ein EMT dem GWA mitteilen, wenn er Anomalien bei den vom SMGW empfangenen Daten feststellt, die auf eine Fehlfunktion oder Kompromittierung hindeuten, oder er (wiederholt) unberechtigte Kommunikation von SMGW feststellt.

Alle diese Vorgaben sind durch ein für den Betrieb entwickeltes Informationssicherheits-Managementsystem (ISMS) umzusetzen. Mehr dazu in Kapitel 4.2 dieses Dokuments.

Neben den organisatorischen Anforderungen gelten für EMT auch **technische Sicherheitsanforderungen,** die in Kapitel 6 der Certificate Policy der SM-PKI definiert werden (Bundesamt für Sicherheit in der Informationstechnik, 2023b). Dazu gehören

- die Erzeugung und Installation von Schlüsselpaaren (privater und öffentlicher Schlüssel für die SM-PKI),
- die Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module,
- die Archivierung öffentlicher Schlüssel und Gültigkeitszeiträume von Zertifikaten und Schlüsselpaaren,
- die Aufbewahrung von Aktivierungsdaten für die Kryptografiemodule sowie
- Sicherheitsanforderungen an die Informationstechnik. Diese betreffen die Trennung von internen und externen Netzwerken, Intrusion-Detection-Systeme, Software-Updates, Logging und Audit-Trails, Dateien, Benutzerverwaltung und den Schutz vor Schadsoftware.

Diese Anforderungen unterscheiden in einigen Aspekten zwischen aEMT und pEMT, wobei in allen Fällen die Anforderungen an aEMT höher sind.

4.1.1 Anforderungen an aEMT

Aktive EMT müssen die Anforderungen erfüllen, die in der Norm ISO/IEC 27001 definiert sind. Die Zertifizierung gemäß ISO/IEC 27001 umfasst alle für die PKI relevanten Geschäftsprozesse und IT-Systeme, also vor allem Beantragung, Empfang und Nutzung von Schlüsseln und Zertifikaten (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 5.1.2). Die Zertifizierung muss auch die Überprüfung beinhalten, dass die Certificate Policy des BSI (Bundesamt für Sicherheit in der Informationstechnik, 2023b) eingehalten wurde.

Aktive EMT müssen über die oben genannten Anforderungen hinaus Verfahrensanweisungen umsetzen, die **Vertreterregelungen** für jede definierte Rolle sowie eine klare **Definition der Verantwortlichkeitsbereiche** der Mitarbeiterinnen und Mitarbeiter umfassen. Darüber hinaus müssen kritische Vorgänge nach dem **Vier-Augen-Prinzip** durchgeführt werden. Dazu gehören die Generierung des Schlüsselpaars, ein Schlüsselwechsel, ein Schlüssel-Backup bei einem defekten Kryptografiemodul sowie generell das Schlüsselmanagement.

4.1.2 Anforderungen an pEMT

Passive EMT müssen ein Sicherheitskonzept erstellen und umsetzen, dass die oben genannten Anforderungen aus der SM-PKI Policy (Bundesamt für Sicherheit in der Informationstechnik, 2023b) erfüllt. Die wesentliche Vereinfachung ist die Tatsache, dass dieses Sicherheitskonzept nicht durch die Norm ISO 27001 überprüft werden muss. Die Certificate Policy definiert keine Anforderungen an pEMT, die nicht auch für aEMT gelten.

4.1.3 Sicherheitskonzepte

Ein Sicherheitskonzept hat den Zweck, die oben beschriebenen Anforderungen, die an alle EMT gestellt werden, in konkrete Maßnahmen für die Organisation zu übersetzen. Dies kann je nach Organisation unterschiedlich sein. Beispiel: Die Certificate Policy schreibt vor, dass Unbefugte keinen Zutritt zu den Betriebsräumen erhalten. Die entsprechende Maßnahme im Sicherheitskonzept könnte ein RFID-Schlüsselsystem sein, das nur bestimmten Beschäftigten Zugang zu den entsprechenden Räumen gewährt. Passive EMT müssen dieses Sicherheitskonzept zur Erfüllung aller Anforderungen erstellen und umsetzen, jedoch nicht

zertifizieren lassen. Aktive EMT müssen das Konzept und die Umsetzung über eine ISO/IEC-27001-Zertifizierung nachweisen.

4.2 Zertifizierungs- und Umsetzungsprozesse

Um nach ISO/IEC 27001 zertifiziert zu werden, muss eine Organisation ein eigenes Informationssicherheits-Managementsystem (ISMS) erstellen und umsetzen. Das ISMS dient dazu, ein überprüfbares Sicherheitsniveau im Umgang mit Informationen zu etablieren. Es umfasst nicht nur rein technische Themen wie Firewall, Virenschutz, Updates etc., sondern auch die Definition von Verantwortlichkeiten, Regelungen zum Zutritt zu Gebäuden des Unternehmens, Risikomanagement und die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit.

Das ISMS muss von der Organisation erarbeitet und umgesetzt werden, wofür in der Regel mehrere Monate notwendig sind. Anschließend wird das ISMS von einer externen Organisation (z. B. dem TÜV) in einem Audit initial überprüft, bevor das Zertifikat ausgestellt wird. Das ISMS wird anschließend in regelmäßigen weiteren Audits überprüft, andernfalls verliert das Zertifikat seine Gültigkeit. Die Zertifizierung nach ISO/IEC 27001 ist also mit Kosten und Aufwand verbunden, die von Organisation zu Organisation stark variieren. Da von einer Zertifizierung wesentliche Teile einer Organisation betroffen sind und entsprechende Sicherheitskonzepte gegebenenfalls mit externen Beratern zunächst erarbeitet werden müssen, ist mit einem Vorlauf von mindestens einigen Monaten bis wenigen Jahren vor der Zertifizierung auszugehen. Es ist damit zu rechnen, dass sich die Kosten für die Zertifizierung – je nach Größe der Organisation und Umsetzungsaufwand – im fünfstelligen Euro-Bereich bewegen.

Da potenzielle EMT wie Netzbetreiber zu den Betreibern kritischer Infrastrukturen gehören, sind sie gemäß § 8a BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) ohnehin verpflichtet, organisatorische und technische Vorkehrungen nach Stand der Technik für ihre IT-Sicherheit zu treffen. Als Nachweis dafür gilt (unter gewissen Rahmenbedingungen) ein ISO/IEC-27001-Zertifikat (Bundesamt für Sicherheit in der Informationstechnik, 2023b). Das bedeutet, dass beispielsweise Netzbetreiber ohnehin vergleichbare Sicherheitsanforderungen erfüllen müssen wie aEMT.

Die Certificate Policy des BSI schreibt vor, dass die ISO/IEC-27001-Zertifizierung alle Geschäftsprozesse und IT-Systeme umfassen muss, die für die SM-PKI relevant sind. Außerdem muss die Zertifizierung explizit überprüfen, dass die Anforderungen aus der SM-PKI Policy eingehalten werden. Es kann also nicht jede nach ISO/IEC 27001 zertifizierte Organisation automatisch als aEMT an der SM-PKI teilnehmen.

4.3 Dienstleister

Es ist in der Certificate Policy der SM-PKI explizit die Möglichkeit erlaubt, dass Dienstleister die eigentliche Aufgabe des EMT übernehmen können (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 1.3.3.4). Für Organisationen, die die SMGW-Infrastruktur insbesondere für die Kommunikation über den CLS-Kanal nutzen möchten, ohne sich nach ISO/IEC 27001 zertifizieren zu lassen, ist diese Dienstleistung eine attraktive Option. Die Organisation (hier Kunde genannt) schließt einen Vertrag mit einem EMT-Dienstleister ab. Der Dienstleister stellt den Endpunkt der Kommunikation über das SMGW und veranlasst häufig auch die entsprechende Konfiguration des SMGW. Auf der HAN-Seite kommt oft ein Kommunikationsadapter des Dienstleisters zum Einsatz, die wiederum Schnittstellen für eine lokale Kunden-App bietet. Der Dienstleister stellt also EMT- und CLS-Einheit zur Verfügung und „überbrückt“ damit die Kommunikation über das

SMGW, wie in Abbildung 8 dargestellt ist. Der Kunde muss also selbst nicht an der SM-PKI teilnehmen, was ihm entsprechende Aufwände erspart.

Für die Sicherheit des Gesamtsystems ist die Kommunikation vom Kunden-Backend zum Dienstleister relevant. Würden die Anforderungen des BSI unverändert auch für diese Kommunikation gelten, wäre keinerlei Vereinfachung erreicht. Andererseits wäre ohne jegliche Sicherheitsanforderungen an diese Kommunikation die Möglichkeit geschaffen, die Sicherheitsanforderungen aus der SM-PKI komplett zu umgehen, da über den Kanal jede Kommunikation möglich wäre. Das BSI schreibt dementsprechend als Mittelweg vor, dass darauf geachtet werden muss, dass die Kommunikation ein mit den kryptografischen Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik, 2022) vergleichbares Sicherheitsniveau aufweist (Bundesamt für Sicherheit in der Informationstechnik, 2023b, Kap. 1.3.3.4). Zertifizierungsprozesse oder Ähnliches sind nicht vorgesehen. Es bleibt selbstverständlich dem Dienstleister erlaubt, bestimmte technische oder organisatorische Vorgaben zu definieren.

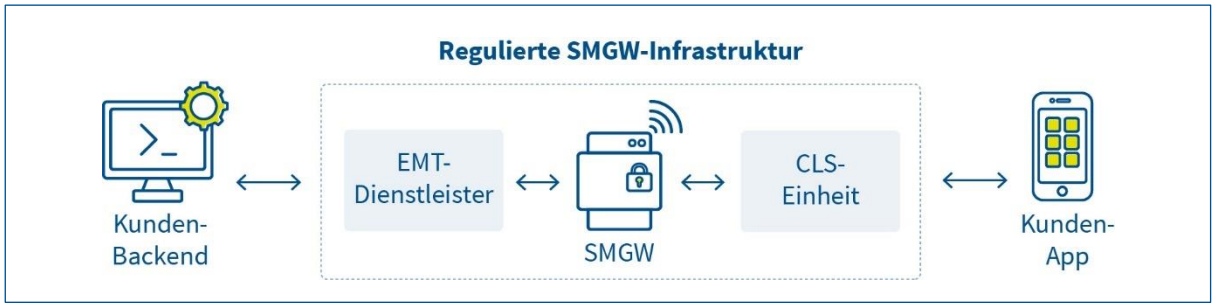

Abbildung 8 Kommunikation über Dienstleister

Es gibt mehrere EMT-Dienstleister am Markt. Ihre Dienstleistung wird oft als „Aktiver EMT as a Service“ oder „CLS-Management“ vermarktet. Manche sind gleichzeitig Messstellenbetreiber oder Gateway-Hersteller, was aufgrund der Unternehmensanforderungen naheliegend ist.

Beispiele für diese Dienstleister sind, ohne Anspruch auf Vollständigkeit und alphabetisch sortiert, in folgender Übersicht zusammengefasst:

Beispiele für EMT/CLS-Dienstleister

- aktiver EMT GmbH
- Auxilius Services GmbH
- meterpan GmbH
- MTG AG
- Voltaris GmbH
- Zenner Connect GmbH

5 Praxisleitfaden und Schlussfolgerungen

Wenn eine Organisation die SMGW-Infrastruktur nutzen möchte, stehen ihr (je nach Anwendungsfall) bis zu vier Optionen zur Verfügung. Für jede Option wird im Folgenden eine zusammenfassende Checkliste für ihre Umsetzung aufgeführt.

Nutzung eines Dienstleisters

Dienstleister ermöglichen Organisationen ohne ISO/IEC-27001-Zertifizierung die Nutzung der SMGW-Infrastruktur.

✓	Sicherstellen, dass die Kommunikation zum Dienstleister ein vergleichbares Sicherheitsniveau aufweist, wie es in der BSI TR-03109-3 definiert ist
✓	Kontaktaufnahme zu einem Dienstleister und Implementierung einer Schnittstelle, die vom Dienstleister genannt wird

Energieserviceanbieter (ESA)

Als ESA kann man Messdaten aus dem Backend des MSB empfangen.

✓	Implementieren einer Schnittstelle, die EDIFACT-Nachrichten nach den Vorgaben des BDEW (Regelungen zum Übertragungsweg) empfangen kann
✓	Kontaktaufnahme zum MSB des Anschlussnutzers oder der Anschlussnutzerin oder des Anschlussnutzes und Buchen des Angebots für ESA
✓	Einholen des Einverständnisses der Anschlussnutzerin oder des Anschlussnutzers zur Verarbeitung der Messdaten zum Beispiel über die Muster-Einwilligungserklärung des BDEW

Passiver EMT (pEMT)

Ein pEMT kann Messdaten aus einem iMSys empfangen und mit anderen Teilnehmern der SM-PKI kommunizieren.

✓	Erstellen eines Sicherheitskonzepts zur Umsetzung der Certificate Policy der SM-PKI
✓	Registrierung bei einer Sub-CA, Nachweis über erfolgreiche Tests mit der Sub-CA
✓	Bestellung der Konfiguration des iMSys bei einem MSB
✓	Implementieren einer Schnittstelle für den Datenempfang aus SMGW nach BSI-TR 03109 unter Verwendung der Schlüssel der SM-PKI (TLS-Server)

Aktiver EMT (aEMT)

Ein aEMT kann den CLS-Kanal des SMGW nutzen, mit anderen Teilnehmenden der SM-PKI kommunizieren und Messdaten aus dem iMSys empfangen.

✓	Erstellen eines Sicherheitskonzepts zur Umsetzung der Certificate Policy der SM-PKI
✓	Zertifizierung der Organisation nach ISO/IEC 27001 mit Nachweis der Einhaltung der Certificate Policy der SM-PKI
✓	Registrierung bei einer Sub-CA, Nachweis über erfolgreiche Tests mit der Sub-CA
✓	Bestellung der Konfiguration des iMSys bei einem MSB
✓	Implementieren einer Schnittstelle für den Datenempfang aus SMGW nach BSI TR-03109 unter Verwendung der Schlüssel der SM-PKI (TLS-Server)

Zusammenfassend lässt sich feststellen, dass die Nutzung der SMGW-Infrastruktur mit einem nicht vernachlässigbaren Aufwand verbunden ist. Die technischen Anforderungen sind insbesondere für Unternehmen im IT-Bereich das geringere Problem. Dagegen machen es vor allem die Zertifizierungs- und Umsetzungsprozesse insbesondere für Start-ups oder junge Unternehmen, die neue Geschäftsmodelle unter Nutzung des SMGW aufbauen wollen, unattraktiv, direkt mit iMSys zu kommunizieren. In der Regel ist hier die Inanspruchnahme eines Dienstleisters die einfachere und auch schnellere Option.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

BDEW (2021): *Regelungen zum Übertragungsweg, Version 1.5*. https://www.edi-energy.de/index.php?id=38&tx_bdew_bdew%5Buid%5D=1275&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=e8ef3726dd6219771d7263f07ef5e57c

Bundesamt für Sicherheit in der Informationstechnik (2017): *BSI TR-03109-4 – Smart Metering PKI – Public Key Infrastruktur für Smart Meter Gateways – Version 1.21.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meterin-PKI/TechnRichtlinie/tr_03109-4_node.html

Bundesamt für Sicherheit in der Informationstechnik (2021): *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*.

Bundesamt für Sicherheit in der Informationstechnik (2022): *Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-3.pdf?__blob=publicationFile&v=9

Bundesamt für Sicherheit in der Informationstechnik (2023a): *Certificate Policy der Smart Metering PKI, Version 1.1.2*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/PKI_Certificate_Policy.pdf?__blob=publicationFile&v=7

Bundesamt für Sicherheit in der Informationstechnik (2023b): *BSI – FAQ Nutzung ISO/IEC 27001 Zertifikat*. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-Nutzung-ISO-27001-Zertifikat/faq-nutzung-iso-27001-zertifikat_node.html

Bundesamt für Sicherheit in der Informationstechnik (2023c): *BSI – SM PKI Root CA.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meterin-PKI/SMPKIRootCA/smpkirootca_node.html

Bundesnetzagentur (2020): *Beschluss Az. BK6-20-160*.
https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2020/BK6-20-160/Bk6-20-160_beschluss_vom_21.12.2020.pdf?__blob=publicationFile&v=1

Bundesnetzagentur (2022a): *Beschluss BK6-22-128 (Universalbestellprozess)*.
https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_83_Zug_Mess/843_universalbestellprozess/BK6_universalbestellprozess_node.html

Bundesnetzagentur: (2022b): *Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (GPKE)*.
https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-128/Anlagen_Beschluss/BK6-22-128_Lese_Anlage1.pdf?__blob=publicationFile&v=1

Bundesnetzagentur: (2022c): *Wechselprozesse im Messwesen Strom (WiM Strom)*.
https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-128/BK6-22-128_Beschluss.html

Wendzel, S. (2018): *IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung*.
Springer Vieweg.

Abkürzungen

aEMT	Aktiver externer Marktteilnehmer
BDEW	Bundesverband der deutschen Energie- und Wasserwirtschaft
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CLS	Controllable Local System
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
ESA	Energieserviceanbieter
FNN	Forum Netztechnik/Netzbetrieb im VDE
GWA	Gateway-Administrator
GWH	Gateway-Hersteller
HAN	Home Area Network
HKS	HAN-Kommunikationsszenario
IEC	International Electrotechnical Commission
iMSys	Intelligentes Messsystem
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
LAN	Local Area Network
LMN	Local Metrological Network
MaKo	Marktkommunikation
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
pEMT	Passiver externer Marktteilnehmer
PKI	Public Key Infrastruktur
RA	Registration Authority
SM-PKI	Smart Metering Public Key Infrastruktur
SMGW	Smart Meter Gateway

TLS	Transport Layer Security
TR	Technische Richtlinie
VDE	Verband Deutscher Elektroingenieure
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

www.dena.de www.set-hub.de