

Sternförmige Kommunikation von Werten Typ 2 mit dem intelligenten Messsystem

Weitergabe von nicht abrechnungsrelevanten Messdaten und Realisierung von CLS-Verbindungen direkt aus dem Messsystem an externe Marktteilnehmer

Inhalt

Vorwort	3
Begriffe und Abkürzungen.....	4
1 Einleitung / Problemstellung.....	5
2 Einheitlicher Lösungsansatz	6
3 Umsetzungsempfehlung	7
3.1 Adressumsetzung für die Kommunikation zu externen EMT	7
3.2 Sicherheitsrelevanz in der Sternverteilung	7
3.2.1 Außerhalb des MSB-Bereiches, andere Marktteilnehmer	7
3.2.2 Innerhalb des MSB-Bereiches, verantwortlicher MSB/GWA	7
3.3 Weitere Aspekte.....	7
3.3.1 Verursachergerechte Erfassung von Datenvolumen.....	7
3.3.2 Unterbrechung von bestehenden Verbindungen.....	7
3.3.3 Verfügbarkeit des Breakout-Gateways	7
4 Aufgaben für die Marktkommunikation.....	8
5 Literaturverzeichnis.....	9

Vorwort

In den Niederspannungsnetzen sind zunehmend steigende Einspeise- und Verbrauchseinrichtungen wie Solaranlagen, Wärmepumpen und Wallboxen zur Ladung von Elektrofahrzeugen im Einsatz, die ins Stromnetz integriert werden müssen. Grundlage dafür ist, dass Verteilnetzbetreiber (VNB) und berechnigte Marktteilnehmer Netzzustandsdaten direkt aus den intelligenten Messsystemen der Messtellenbetreiber (MSB) benötigen. Dies ist ein wichtiger Baustein zur Steuerung der Anlagen durch die aktiven Marktteilnehmer (aEMT) und für die Möglichkeit des Eingriffes durch Netzbetreiber zur stabilen Bereitstellung der Stromversorgung. Ferner benötigen Dienstleister Zugang über das Smart Meter Gateway (SMGW) per Controllable Local System (CLS) zu angeschlossenen Anlagen und Submetersystemen.

Dieser VDE FNN Hinweis zeigt eine Systemarchitektur auf, mit der MSB die sichere Datenkommunikation zwischen intelligenten Messsystemen und externen aktiven und passiven Marktteilnehmern (EMT) ermöglichen können.

Begriffe und Abkürzungen

aEMT	Aktiver Marktteilnehmer - kann über ein intelligentes Messsystem mit einer Anlage kommunizieren
API	Application Programming Interface oder Programmierschnittstelle
APN	Access Point Name – Zugangspunkt, Netzwerkpfad
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BNetzA	Bundesnetzagentur
Breakout-Gateway	Zugangspunkt zum Internet
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLS	Controllable Local System
EMT	Externer Marktteilnehmer (aktiv und/oder passiv)
GWA	Gateway Administration
IP-Accounting	Aufzeichnung der Anzahl Bytes und Pakete je IP-Adresse (Transitverkehr)
IPv4	Internet Protocol Version 4 - wurde in RFC 791 im Jahr 1981 definiert
IPv6	Internet Protocol Version 6 - seit 1998 standardisiertes Verfahren zur Übertragung von Daten in paketvermittelnden Rechnernetzen
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
NAT	Network Address Translation, Adressenübersetzung in IT-Netzen
pEMT	Passiver Marktteilnehmer – kann Daten aus einem intelligenten Messsystem empfangen
RFC	Requests for Comments – Standards der Internetprotokoll-Familie
SMGW	Smart Meter Gateway – Kernbestandteil eines intelligenten Messsystems
Stateful	Zustandsbehaftet – ermöglicht bei einer Firewall den Eingang von Daten über eine zuvor ausgehende Verbindung
TLS	Transport Layer Security – Sicherheitsprotokoll
VNB	Verteilnetzbetreiber
VPN	Virtual Private Network, Virtuelles Privates Kommunikationsnetz

1 Einleitung / Problemstellung

Mit intelligenten Messsystemen wird das Ziel verfolgt, eine sichere Datenkommunikation mit den Liegenschaften zu etablieren. Für abrechnungs- bilanzierungsrelevante Daten spielt eine sternförmige Kommunikation aus dem Smart Meter Gateway keine Rolle, da diese über den MSB übermittelt werden, um z.B. Ersatzwertbildung im Backend System des MSB zu ermöglichen.

In § 34 Messstellenbetriebsgesetz (MsbG) wurde festgelegt, dass der MSB auch Standard- und Zusatzleistungen über sternförmige Kommunikation anbieten muss [1]. Zu den Standardleistungen zählen vor allem der tägliche Versand von Netzzustandsdaten an den VNB sowie die Lieferung von Werten zur Ist-Einspeisung gemäß MsbG. Als Zusatzleistungen sind z. B. der minütliche Versand von Netzzustandsdaten an den VNB sowie die Bereitstellung von abrechnungsrelevanten Messdaten aus Submetering-Systemen zu nennen.

Die Bestellung der Leistungen erfolgt über die Marktprozesse der Bundesnetzagentur (BNetzA) [3], [4], [5], [6]. Die auftraggebende Marktrolle kann hierbei Bestellungen für Konfigurationen aus der „Codeliste der Konfigurationen“ wählen.

Die direkte Adressierung der Kommunikationssysteme der Marktteilnehmer ist funktional im SMGW umgesetzt [7]. Da SMGW in der Regel in privaten Kommunikationsnetzen des MSB betrieben werden, muss für die sternförmige Kommunikation ein Routing ins Internet ermöglicht werden. Dieses Dokument soll MSB dabei unterstützen, hier eine Lösung auszuprägen, die auch zukünftige Anforderungen mit abdeckt.

2 Einheitlicher Lösungsansatz

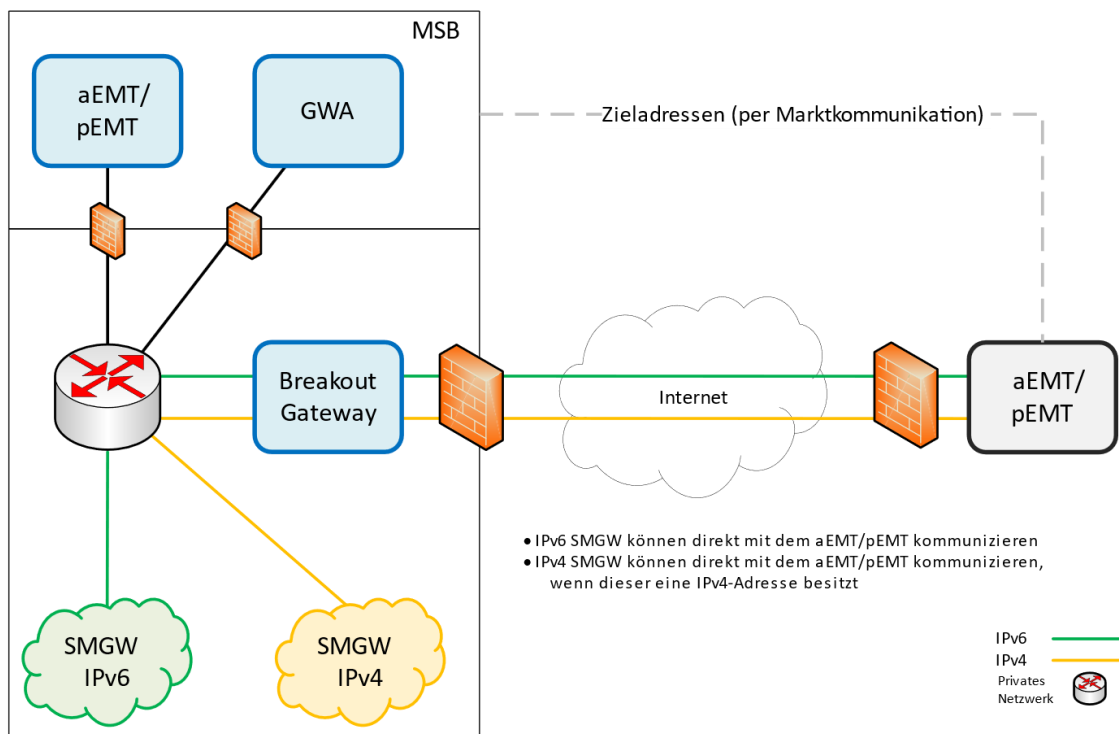


Abbildung Einheitlicher Lösungsansatz (Architektur)

In der Abbildung dargestellten Referenz-Netzwerk-Architektur sind die SMGW in einem privaten Netzwerk verortet. Dabei spielt es keine Rolle, welche Telekommunikationstechnologie zur Anbindung der SMGW verwendet wird. Die dargestellte Architektur kann sinngemäß mit allen Kommunikationstechnologien umgesetzt werden. Die Anbindung kann beispielsweise über einen privaten APN eines Mobilfunk-Anbieters oder über Breitband Powerline Netze realisiert werden.

Die SMGW können dabei sowohl mit IPv4 als auch mit IPv6 [2] betrieben werden, wobei VDE FNN die Verwendung von globalen IPv6-Adressen im Sinne einer durchgängigen Infrastruktur und aufgrund der betrieblichen Vorteile empfiehlt.

Die Systeminfrastruktur des MSB ist dabei mit Gateway-Administrations- (GWA) und dem eigenen EMT-System beispielsweise über einen VPN-Kanal direkt an dieses Netzwerk angebunden. Dadurch kann der GWA die SMGW unmittelbar erreichen und den Aufbau eines Kommunikationskanals zum EMT durch die Übermittlung eines Wake-up-Pakets initiieren.

Die Kommunikation zu EMT-Systemen wird grundsätzlich immer vom SMGW initiiert. Das SMGW kann somit den EMT des MSB in diesem Netzwerk unmittelbar erreichen, um Messdaten zu übermitteln oder einen CLS-Kommunikationskanal aufzubauen.

Die Kommunikation zu den EMT-Systemen Dritter ist ebenfalls möglich. Über ein Breakout-Gateway wird eine Anbindung ans öffentliche Internet realisiert, wobei der MSB die Kommunikation per Firewall-Konfiguration auf ausgehenden Traffic beschränken und ggf. weitere Einschränkungen wie z. B. die Begrenzung des Datenvolumens/Datendurchsatzes vornehmen kann, die die Sicherheit seiner Infrastruktur erhöhen.

3 Umsetzungsempfehlung

Bei der Umsetzung sind Adressierung und Sicherheitsaspekte zu berücksichtigen.

3.1 Adressumsetzung für die Kommunikation zu externen EMT

Ein EMT-System eines Dritten muss grundsätzlich über eine global gültige IPv6-Adresse erreichbar sein. Sollte Datenkommunikation mit IPv4-SMGW erfolgen, muss zusätzlich eine global gültige IPv4-Adresse bereitgestellt werden. Diese Adresse und weitere Konfigurationsparameter werden dem MSB idealerweise per Marktkommunikation übermittelt und dann von diesem als Zieladresse im SMGW hinterlegt.

In der Regel nutzen IPv4-SMGW einen privaten IP-Adressbereich. Somit müssen diese am Breakout-Gateway per NAT auf eine öffentliche IP-Adresse umgesetzt werden. Der EMT benötigt daher eine öffentliche IPv4-Adresse.

3.2 Sicherheitsrelevanz in der Sternverteilung

3.2.1 Außerhalb des MSB-Bereiches, andere Marktteilnehmer

Die öffentlich erreichbare Adresse eines EMT-Systems eines Dritten ist über eine Firewall zu schützen. In der Firewall kann beispielsweise beim Betrieb der SMGW über IPv6 auf die zu erwartende IP-Range der SMGW gefiltert werden. Beim Betrieb der SMGW über IPv4 kann die Kommunikation auf die Adresse des Breakout-Gateways beschränkt werden, die durch das vorgenommene NAT als einzige Adresse nach außen sichtbar ist. Die Einschränkung auf die verwendeten Kommunikations-Ports sollte ebenfalls gesetzt werden. Die Kommunikation ist mit TLS zu verschlüsseln.

3.2.2 Innerhalb des MSB-Bereiches, verantwortlicher MSB/GWA

Generell wird der Verbindungsaufbau durch das SMGW initiiert. Der Rückweg der Kommunikation wird durch die Stateful Funktion der Firewall gewährleistet. Intern sind die IPv6-Adressen des externen Marktteilnehmers entsprechend in der Firewall freizuschalten. Die IPv4-Adressen sind über einen NAT auf eine öffentliche IPv4-Adresse umzusetzen.

Die Dimensionierung von Firewall, Breakout-Gateway und NAT-Funktionen sollten so erfolgen, dass der vorgesehene Datenverkehr ohne Verzögerungen umgesetzt werden kann.

Weiterhin sollen die einschlägigen Empfehlungen des BSI Berücksichtigung finden [8].

3.3 Weitere Aspekte

3.3.1 Verursachergerechte Erfassung von Datenvolumen

Bei zukünftigen Anforderungen kann es notwendig werden, das Datenvolumen je Empfänger bzw. je Transportverbindung zu erfassen. Hierzu kann im Breakout-Gateway eine IP-Accounting-Funktion vorgesehen werden.

3.3.2 Unterbrechung von bestehenden Verbindungen

Das Breakout-Gateway muss bestehende Verbindungen eines oder mehrerer SMGW zu EMT unterbrechen können. Hierzu wird eine API-Verbindung des GWA zum Breakout-Gateway bzw. zu dessen Administration benötigt.

3.3.3 Verfügbarkeit des Breakout-Gateways

Um eine sichere Kommunikation möglichst auch im Störfall abzusichern, sind für Hard- und Software entsprechende Redundanzen oder Ausweichverfahren vorzusehen. Die Redundanzen sind bei der Bekanntgabe der IP-Adressen entsprechend zu berücksichtigen.

4 Aufgaben für die Marktkommunikation

Im Rahmen des Datenaustausches zwischen MSB und EMT über die Marktkommunikation müssen die IP Adressen für die Kommunikation zwischen dem intelligenten Messsystem und EMT vereinbart werden:

Die Vereinbarung von IP-Adressen oder IP Address Ranges kann durch:

- den Besteller in Richtung MSB
 - Vereinbarung einer IPv4- oder IPv6-Adresse je SMGW im Universalbestellprozess,
- oder
- den MSB in Richtung Besteller
 - Vereinbarung von IP-Ranges für SMGW (IPv6-Adressen)
 - Vereinbarung von IP-Ranges für SMGW (öffentliche IPv4-Adressen)
 - Vereinbarung von IP-Adresse/IP-Ranges für Breakout-Gateway/NAT-Service (öffentliche IPv4 Adressen)

erfolgen.

Solange diese Vereinbarung nicht im Universalbestellprozess möglich ist, ist die Vereinbarung zwischen den MSB und Besteller bilateral vorzunehmen.

5 Literaturverzeichnis

- [1] Messstellenbetriebsgesetz (MsbG), Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen.
- [2] IETF, „About RFCs“ , Online. Available: <https://www.ietf.org/process/rfc/>. [Zugriff am 03.05.2024].
- [3] BDEW, „Aktuell gültige Dokumente“, Online. Available: <https://www.edi-energy.de/index.php?id=38>. [Zugriff am 03.05.2024].
- [4] BDEW, „BDEW-Anwendungshilfe „Rollenmodell für die Marktkommunikation im deutschen Energiemarkt“ (Version 2.1), Online. Available: <https://www.bdew.de/service/anwendungshilfen/rollenmodell-fuer-die-marktkommunikation-im-deutschen-energiemarkt/>. [Zugriff am 03.05.2024].
- [5] BDEW, VDE FNN, „BDEW/FNN-Anwendungshilfe VDE-AR-N 4400 – Marktkommunikation: Zusammenwirken von Messtechnik und Marktkommunikation“, Online. Available: <https://www.vde.com/de/fnn/arbeitsgebiete/digitalisierung-metering/metering-code-vde-ar-n-4400>. [Zugriff am 03.05.2024]
- [6] BNetzA, „Festlegung zur prozessualen Abwicklung von Steuerungshandlungen in Verbindung mit intelligenten Messsystemen (iMS) (Universalbestellprozess)“, Online. Available: https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_83_Zug_Mess/843_universalbestellprozess/BK6_universalbestellprozess_node.html. [Zugriff am 03.05.2024]
- [7] VDE FNN, „Smart-Meter-Gateway: Die Zentraleinheit des intelligenten Messsystems“, Online. Available: <https://www.vde.com/de/fnn/arbeitsgebiete/digitalisierung-metering/lastenhefte/smart-meter-gateway>. [Zugriff am 03.05.2024]
- [8] BSI, „BSI-Standards zur Internet-Sicherheit (ISi-Reihe)“, Online. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISi-Reihe/isi-reihe_node.html. [Zugriff am 03.05.2024].

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.

Forum Netztechnik/Netzbetrieb im VDE (FNN)
Bismarckstraße 33
10625 Berlin
Tel. +49 30 383868-70
fnn@vde.com
www.vde.com/fnn