CASA

Produkthandbuch für das Smart Meter Gateway CASA 1.0 und CASA 1.1

- FÜR LETZTVERBRAUCHER

CASA-PHB-LV-D-2.03
Stand: 15.05.2025
DE

EMH ist nach der DIN EN ISO 9001:2015 zertifiziert und bemüht sich ständig um die Verbesserung der Produkte.

Der Inhalt dieses Handbuchs und die technischen Spezifikationen können ohne vorherige Ankündigung ergänzt, geändert oder entfernt werden.

Die Beschreibung der Produktspezifikation in diesem Handbuch stellt keinen Vertragsbestandteil dar. Technische Änderungen und Irrtum vorbehalten.

Bei Fragen oder Anregungen erreichen Sie uns unter:

EMH metering GmbH & Co. KG

Neu-Galliner Weg 1
19258 Gallin / DEUTSCHLAND

Telefon: +49 38851 326-0
Fax: +49 38851 326-1129

E-Mail: info@emh-metering.com
Internet: www.emh-metering.com

Technischer Support:

Telefon: +49 38851 362-1930
E-Mail: support@emh-metering.com

Hinweise zum Produkthandbuch

Dieses Produkthandbuch ist Teil der Dokumentation des Smart Meter Gateway CASA.
Es enthält notwendige Informationen zum sicheren Gebrauch. Lesen Sie diese Anleitung vor Beginn aller Arbeiten aufmerksam durch. Bewahren Sie dieses Produkthandbuch sowie alle anderen mitgelieferten Unterlagen sorgfältig auf, damit sie während der gesamten Lebensdauer des Gerätes zur Verfügung stehen.

Aus Gründen der Lesbarkeit wird in diesem Dokument für Personen ausschließlich die männliche Form verwendet. Gemeint sind Personen jeglicher Geschlechtsidentität.

Zielgruppe

Dieses Produkthandbuch wendet sich an Letztverbraucher (LV).

Das Gerät darf ausschließlich von ausgebildeten Elektrofachkräften nach den allgemein anerkannten Regeln der Technik und gegebenenfalls den Bestimmungen, die für das Errichten von Fernmeldeeinrichtungen und -endgeräten maßgebend sind, installiert und in Betrieb genommen werden.

Geltungsbereich

Dieses Handbuch berücksichtigt alle Ausführungsvarianten und Funktionen des Gerätes. Beachten Sie, dass die Geräte in Bezug auf Konfiguration, Datenschnittstellen, Ein-/Ausgänge u. a. unterschiedlich ausgeführt sein können. Möglicherweise sind daher Merkmale beschrieben, die auf das von Ihnen eingesetzte Gerät nicht zutreffen.

Abbildungen in diesem Produkthandbuch dienen dem besseren Verständnis und können von der tatsächlichen Ausführung des CASA abweichen.

Verwendete Symbole

Die folgende Übersicht erklärt die Bedeutung der in diesem Handbuch verwendeten Piktogramme und Signalwörter.

GEFAHR
bezeichnet eine unmittelbar drohende Gefahr. Wenn sie nicht gemieden wird, sind Tod oder schwerste Verletzungen die Folge.

WARNUNG
bezeichnet eine Gefährdung mit mittlerem Risikograd. Wenn sie nicht gemieden wird, können Tod oder schwere Verletzungen die Folge sein.

HINWEIS
kennzeichnet wichtige Informationen im Produkthandbuch.

JURISTISCHER HINWEIS
kennzeichnet wichtige Informationen im Produkthandbuch.

ARBEITSSCHRITT
Eine Aktion ist erforderlich, z. B. „Drücken einer Taste“ oder „Eingabe eines Wertes“.

TIPP / HINWEIS
Macht auf eine besondere Situation aufmerksam oder gibt einen Tipp zur Funktion.

Dokumentationskonzept

Die Produktdokumentation zum Smart Meter Gateway CASA besteht aus dem Datenblatt, der Gebrauchsanleitung und dem Produkthandbuch.

Hinweise zur Prüfung der Integrität der Dokumentation liegen im Kapitel 1.9 / Seite 9 vor.

- Das Datenblatt beschreibt die unterschiedlichen Ausführungsvarianten des Gerätes und gibt Aufschluss über die Technischen Daten und Merkmale des Produktes.
- Die Gebrauchsanleitung beschreibt den sicheren Umgang mit dem Smart Meter Gateway und den dazugehörigen Komponenten von der Installation bis zur Inbetriebnahme und Entsorgung. Anleitung und Warnhinweise sind unbedingt zu beachten.
- Das Produkthandbuch für Servicetechniker (ST) und Gateway-Administratoren (GWA) wendet sich an Spezialisten, zu deren Aufgaben die Konfiguration und Wartung der intelligenten Messsysteme im Normal- bzw. Wirkbetrieb und bei Auffälligkeiten gehören.
- Das Produkthandbuch für Letztverbraucher (LV) enthält alle Informationen, die für die Nutzung eines bereits installierten und in Betrieb genommenen CASA erforderlich sind.

Dokumentation zu diesem Produkt

Benennung	Dokumentenbezeichnung
Smart Meter Gateway CASA Datenblatt	CASA-DAB-D
Smart Meter Gateway CASA Gebrauchsanleitung	CASA-BIA-D
Smart Meter Gateway CASA Produkthandbuch für Servicetechniker und Gateway-Administratoren	CASA-PHB-ST-GWA-D
Smart Meter Gateway CASA Produkthandbuch für Letztverbraucher	CASA-PHB-LV-D
SMGW-Schnittstellenbeschreibung (CASA API)	CASA_API-SMGW-D

Dokumentation im Internet:

*Weitere Informationen finden Sie auf der Internetseite www.emh-metering.com im Bereich **„Produkte & Lösungen“** bei der Produktbeschreibung zum Smart Meter Gateway.*

Inhaltsverzeichnis

Hinweise zum Produkthandbuch III
Zielgruppe III
Geltungsbereich III
Verwendete Symbole III

Dokumentationskonzept IV
Dokumentation zu diesem Produkt IV

Inhaltsverzeichnis V

1 Zu Ihrer Sicherheit 7
1.1 Grundlegende Sicherheitshinweise 7
1.2 Spezielle Sicherheitsmaßnahmen für den CASA 7
1.3 Bestimmungsgemäßer Gebrauch 8
1.4 Wartungs- und Gewährleistungshinweise 8
1.5 Pflegehinweise 8
1.6 Entsorgung 8
1.7 Länderspezifische Hinweise zum Messbetrieb 9
1.8 Nachvollziehen der Tarifierung und Abrechnung 9
1.9 Integritätssicherung der Dokumentation 9

2 Gerätebeschreibung 10
2.1 Kurzbeschreibung 10
2.2 Technische Daten 11
2.3 Gehäuse- und Anzeigeelemente 13
2.3.1 LED-Anzeige 13
2.3.2 LEDs Schnittstellen 14
2.4 Beschriftung des Gerätes – CASA 1.0 15
2.5 Beschriftung des Gerätes – CASA 1.1 16
2.6 CASA mit Mehrwertmodul 18
2.7 Kommunikationsschnittstellen 18
2.7.1 LMN-Schnittstellen 18
2.7.2 HAN-Schnittstelle 18
2.7.3 [HAN] CLS-Schnittstelle 18
2.7.4 WAN-Schnittstellen 19
2.8 Fehlerzustände 19
2.8.1 Soft Lock-Down Modus 19
2.8.2 Hard Lock-Down Modus 19
2.9 Funktionen 20
2.9.1 Tarifanwendungsfälle 20
2.9.2 Logbücher 22
2.9.2.1 Letztverbraucher-Log 23
2.9.2.2 System-Log 23
2.9.2.3 Eich-Log 23
2.10 Firmware-Update 23

3 Prüfung der Integrität des CASA 24
3.1 CASA Sicherheitssiegel 24
3.1.1 EMH Sicherheitssiegel 24
3.1.2 Unbeschädigtes Sicherheitssiegel 26
3.1.3 Beschädigtes Sicherheitssiegel 26

4 Prozessuale Sicherheit 28
4.1 Internes Sicherheitskonzept des CASA 28
4.1.1 Softwaresicherheitskonzept 28
4.1.2 Schutz der gespeicherten Messwerte gegen Verfälschung 28
4.1.3 Schutz des Programmcodes 28
4.1.4 Schutz von übertragenen und gespeicherten Daten 28
4.1.5 Fehlerereignisse der Zählerdaten 29
4.1.6 Kommunikationsprotokolle und Profile 29
4.1.7 Inhaltsdatensicherung und Signaturbildung 29
4.1.8 Pseudonymisierung von Daten 29
4.2 Organisatorische Hinweise 30
4.2.1 Rollenkonzept 30
4.2.2 Identifizierung und Authentifizierung 31

5 Nutzung des CASA durch den Letztverbraucher 32
5.1 Kommunikationsverbindung mit CASA Benutzerportal einrichten 32
5.2 CASA-Benutzerportal – Übersicht 34
5.3 CASA-Benutzerportal – Benutzerlog 35
5.4 CASA-Benutzerportal – Messwertliste 36
5.4.1 Info 36
5.4.2 Abrechnung 37
5.4.3 Erfassung 38
5.4.4 Tageswerte 39
5.5 CASA-Benutzerportal – Signatur-Zertifikat 39
5.6 CASA-Benutzerportal – Selbsttest 40
5.7 CASA-Benutzerportal – Logout 40
5.8 Fehlerzustand 41

6 Anhang 42
6.1 CASA-Software 42
6.2 Protokollierte Ereignisse 42
6.2.1 LMN 42
6.2.2 HAN-Schnittstelle + CLS-Gerät 42
6.2.3 Operative Betriebsbereitschaft 43
6.2.4 Zeitsynchronisation 43
6.2.5 Selbsttest 43
6.2.6 Messwertübertragung 44
6.2.7 Funktionsüberprüfung 44
6.2.8 Profilkonfiguration 45
6.2.9 Messwertverarbeitung 45
6.3 Herstellerspezifische Fehlercodes 46
6.4 Konformitätserklärungen 55
6.5 Normen und Richtlinien 56
6.6 Abkürzungsverzeichnis 57

1 Zu Ihrer Sicherheit

In diesem Kapitel erhalten Sie Informationen zur Verantwortlichkeit für den sicheren Umgang mit dem Gerät und allgemein gültige Sicherheitsregeln.

1.1 Grundlegende Sicherheitshinweise

Beachten Sie unbedingt die folgenden Hinweise:

WARNUNG

Der Funksender des CASA kann elektronische Geräte wie z. B. Herzschrittmacher in ihrer Funktion beeinträchtigen!

- Beachten Sie die Hinweisschilder und betreiben Sie das Gerät nicht in einem Bereich, in dem ein Mobilfunkverbot gilt.
- Informieren Sie sich ggf. beim zuständigen Arzt oder Hersteller der Geräte.

WARNUNG

Mögliche gesundheitliche Auswirkungen durch elektromagnetische Felder bei erheblicher Expositionsdauer!

Zur Einhaltung der empfohlenen Grenzwerte für die Exposition von Personen gegenüber elektromagnetischen Feldern entsprechend 1999/519/EG muss ein Abstand von mindestens 35 cm zur Antenne eingehalten werden.

- Lesen Sie alle beiliegenden Anleitungen und Informationen.
- Beachten Sie die Warnungen an den Geräten und in den Dokumenten.
- Führen Sie die Bedienung am Gerät stets sicherheits- und gefahrenbewusst aus.
- Verwenden Sie das Gerät nur in technisch einwandfreiem Zustand und ausschließlich im Sinne der bestimmungsgemäßen Verwendung.
- Beachten Sie die Wartungs- und Gewährleistungshinweise.
- Bei Netzausfall und Netzwiederkehr sind keine Handlungen am CASA notwendig.

1.2 Spezielle Sicherheitsmaßnahmen für den CASA

Um die hohen Sicherheitsanforderungen an den Transport, die Installation und den Betrieb des CASA zu erfüllen, müssen die nachfolgend aufgezählten Bedingungen erfüllt bzw. Maßnahmen getroffen werden.

§ Wenn die nachfolgend genannten Bedingungen für den Umgang mit dem CASA nicht erfüllt sind, darf das Gerät aufgrund behördlicher Vorgaben nicht verwendet werden!

1. Der CASA muss in einer nichtöffentlichen Umgebung in den Räumlichkeiten des Letztverbrauchers (LV) installiert werden. Der Installationsort muss mit einem Grundniveau an physischem Schutz ausgestattet sein, wobei der Schutz sich auf den CASA und den mit ihm kommunizierenden Zähler erstreckt.
2. Nur autorisierte Personen dürfen physischen Zugang zum CASA haben.

3. Im vorliegenden Dokument beziehen sich die gegebenen konkreten Informationen oder Handlungsanweisungen zum CASA immer auf einen autorisierten Benutzer:
   - den autorisierten Gateway-Administrator (GWA),
   - den autorisierten Servicetechniker (ST),
   - den autorisierten Letztverbraucher (LV),
   - den autorisierten Messstellenbetreiber (MSB),
   - den autorisierten externen Marktteilnehmer (EMT)

   Dies gilt auch dann, wenn im Text die Rollenbezeichnung ohne den Zusatz „autorisiert“ angegeben ist.

1.3 Bestimmungsgemäßer Gebrauch

Der CASA ist ausschließlich für die Erfassung und Übertragung von Messdaten in Verbindung mit zugelassenen Messgeräten gemäß der technischen Beschreibung und nach ordnungsgemäßer Installation zu verwenden. Der CASA darf nicht außerhalb der spezifizierten technischen Daten betrieben werden (siehe Leistungsschild).

Stellen Sie sicher, dass das Gerät für den vorgesehenen Einsatzzweck geeignet ist.

1.4 Wartungs- und Gewährleistungshinweise

Das Gerät ist wartungsfrei. Bei Schäden (z. B. durch Transport, Lagerung) dürfen selbst keine Reparaturen vorgenommen werden. Falls ein Mangel auf äußere Einflüsse zurückzuführen ist (z. B. Blitz, Wasser, Brand, extreme Temperaturen und Witterungsbedingungen), sowie bei unsachgemäßer oder nachlässiger Verwendung bzw. Behandlung, erlöschen der Gewährleistungsanspruch, die Konformitätserklärung und die Zertifizierung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI).

§ *Beim Öffnen des Gerätes erlöschen der Gewährleistungsanspruch, die Konformitätserklärung und die Zertifizierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI).*
Gleiches gilt für Beschädigung oder Entfernung des Sicherheitssiegels.

1.5 Pflegehinweise

GEFAHR

Das Berühren unter Spannung stehender Teile ist lebensgefährlich!

Zur Reinigung des Gehäuses des CASA müssen alle Leiter, an die der CASA angeschlossen ist, spannungsfrei sein.

Reinigen Sie das Gehäuse des Gerätes mit einem trockenen Tuch.
Verwenden Sie keine chemischen Reinigungsmittel!

1.6 Entsorgung

Das Symbol der durchgestrichenen Abfalltonne auf Elektro- und Elektronikgeräten weist darauf hin, dass das jeweilige Gerät nach der Außerbetriebnahme getrennt vom unsortierten Siedlungsabfall zu entsorgen ist.

Weitere Entsorgungshinweise finden Sie auf der Webseite des Herstellers: www.emh-metering.com.

1.7 Länderspezifische Hinweise zum Messbetrieb

In diesem Abschnitt sind Hinweise und Vorgaben für den Messbetrieb aufgeführt. Diese wurden von der notifizierten Stelle (Modul B) aus dem nationalen Konformitätsbewertungsverfahren vorgegeben und sind durch den Verwender zu beachten. Weitere nationale Rechtsvorschriften zum Messbetrieb bleiben davon unberührt und sind weiterhin zu berücksichtigen.

Deutschland (Messrichtigkeitshinweise)

Für eine mess- und eichrechtskonforme Verwendung des CASA müssen die Angaben im Dokument „Betriebshinweise für eine mess- und eichrechtskonforme Verwendung“ beachtet und umgesetzt werden.

1.8 Nachvollziehen der Tarifierung und Abrechnung

Entsprechend der Vorgaben des Mess- und Eichrechts muss es dem Letztverbraucher ermöglicht werden, die auf Basis der Messwerte des SMGW zustandegekommene Abrechnung (Tarifrechnung) seines Lieferanten nachzuvollziehen.

Im Falle des CASA erfolgt dies unter Zuhilfenahme der Transparenz- und Display-Software (TRuDI), die von der PTB für diesen Zweck bereitgestellt wird:

https://www.ptb.de/cms/ptb/fachabteilungen/abt2/fb-23/ag-234/info-center-234/trudi.html

1.9 Integritätssicherung der Dokumentation

Zur Absicherung gegen unautorisierte Modifikationen der CASA-Handbücher sind für die Dokumente auf den Webseiten der EMH metering kryptografische Prüfsummen nach dem Secure Hash Algorithm SHA256 hinterlegt.

Der Begriff „Secure Hash Algorithm“ (SHA) bezeichnet eine Gruppe standardisierter kryptografischer Hashfunktionen. Diese dienen zur Berechnung einer Prüfsumme (Hash-Wert) für Daten und Dokumente.

Die hinterlegten Hash-Werte können von jedem Nutzer der Handbücher zur Integritätsprüfung verwendet werden.

Die Hash-Werte für die Benutzerdokumente zum CASA sind in diesem Dokument aufgeführt:

„CASA 1.0 und CASA 1.1 – Security Target (CASA-ST)“

Dieses Dokument ist Bestandteil des Common-Criteria-Zertifizierungsverfahrens mit der ID BSI-DSC-CC-0919V4 beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Das aktuelle Security Target Dokument kann von den Webseiten des BSI heruntergeladen werden. Hierzu finden Sie einen Download-Link auf den Webseiten der EMH metering im Bereich „Produkte und Lösungen“ bei der Produktbeschreibung des Smart Meter Gateway.

Die Hash-Werte können mit der Software Gnu Privacy Guard (GPG) oder vergleichbarer Software geprüft werden. Die Software Gnu Privacy Guard (GPG) kann von folgender Webseite heruntergeladen werden:
https://www.gpg4win.org/

In dem GPG-Paket ist das Programm „Kleopatra“ enthalten, mit dem die Hash-Werte für die Prüfung erzeugt werden können.

Nach der Installation kann im Windows-Explorer über das Kontextmenü mit der rechten Maustaste die Datei ausgewählt werden, zu welcher der Hash-Wert erzeugt werden soll.

Als Ergebnis wird eine Datei **„sha256.txt“** erzeugt, in welcher der Hash-Wert enthalten ist.

Der erzeugte Hash-Wert muss mit dem auf der EMH-Webseite angegebenen Wert verglichen werden. Sind beide Werte identisch, wurde das Dokument, für das der Hash-Wert erzeugt wurde, nicht verändert.

2 Gerätebeschreibung

2.1 Kurzbeschreibung

CASA: Akronym für „Communication access security administrator“

Der CASA ist eine eichpflichtige Kommunikations- und Zusatzeinrichtung für intelligente Messsysteme, zugelassen durch die Physikalisch-Technische Bundesanstalt (PTB) und zertifiziert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Hardware- und Softwarekomponenten sind so kombiniert und konfiguriert, dass alle Daten der angeschlossenen Zähler den Anforderungen entsprechend registriert, gespeichert und weitergeleitet werden. Die Weiterleitung der Daten kann an die Zentrale des Messstellenbetreibers (MSB) oder an einen externen Marktteilnehmers (EMT) wie z. B. ein Energieversorgungsunternehmen erfolgen.
Mit der Bereitstellung der Messdaten sind diese für Abrechnungszwecke verfügbar.

Des Weiteren sichert der CASA die Kommunikationsverbindungen zwischen steuerbaren Geräten und externen Marktteilnehmern. Ein Beispiel hierfür wäre die Steuerung dezentraler Energieerzeuger und flexibler Lasten.

Der CASA erhält die gemessenen Zählerstände von unterschiedlichen Zählern wie etwa Stromzähler, Wasserzähler, Gaszähler, Wärmezähler etc. Nach den Vorgaben des Versorgungsvertrags des Letztverbrauchers (Endkunden) mit den Versorgungsunternehmen werden die Messwerte gesammelt, signiert und gespeichert, um anschließend über eine WAN-Schnittstelle an berechtigte Marktteilnehmer versendet zu werden. Auf diese Weise erhält bspw. der Versorger die Daten zur Abrechnung.

Zudem kann der Letztverbraucher über die HAN-Schnittstelle Verbrauchsdaten bzw. kann der Servicetechniker Systeminformationen abrufen. Die Systeminformationen beziehen sich u. a. auf die Kommunikation über die WAN- und LMN-Schnittstelle.

2.2 Technische Daten

Die Daten in der nachfolgenden Tabelle beziehen sich auf den CASA 1.0 und auf den CASA 1.1.

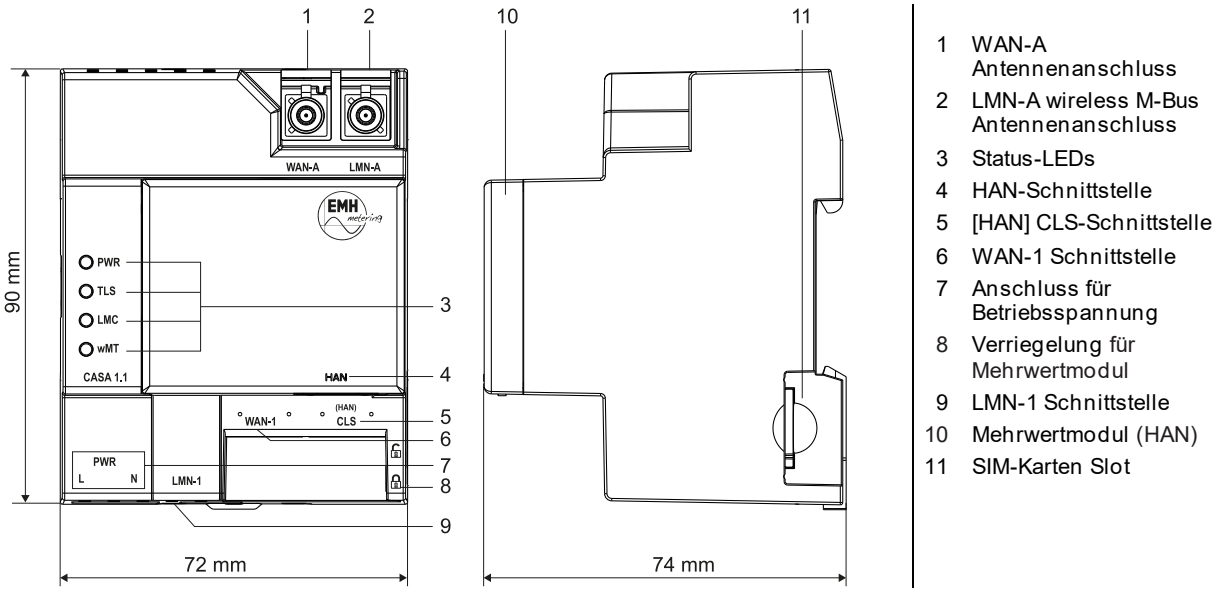
Versorgung	Spannung Strom Frequenz	230 V AC max. 100 mA 50 Hz
Echtzeituhr	Gangreserve	48 h
Anzeigen	4 LEDs	Basisanzeige nach FNN: PWR – Power TLS – Transport Layer Security LMC – Local Meter Controller wMT – Wireless M-Bus Traffic Zusätzlich werden im vorpersonalisierten Zustand Informationen zum Installationsstatus angezeigt.
Geräteschnittstellen (je nach Geräteausführung)	Zählerschnittstellen Kundenschnittstellen Weitbereichsschnittstellen	LMN-1, LMN-A HAN, [HAN] CLS WAN-1, WAN-A
LMN-1 RS485	Ausgangsspannung Strombelastbarkeit Übertragungsrate Anschluss	12 V DC ±5 % max. 290 mA 921,6 kBit/s 6P6C-Buchse (RJ12)
LMN-A Wireless M-Bus	Wireless M-Bus Anschluss	ISM / 868,95 MHz Mode T/C (gemäß EN 13757-4 inkl. OMS TR 07 Kompaktprofil nach BSI TR-03109-1-Detailspezifikation) FAKRA-Stecker, C-codiert, blau
HAN Ethernet	Ethernet Anschluss	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i) 8P8C-Buchse (RJ45)
[HAN] CLS Ethernet	Ethernet Anschluss	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i) 8P8C-Buchse (RJ45)
WAN-A LTE (Fallback GPRS)	Frequenzbereich Ausgangsleistung Anschluss	LTE-Modul (B20 / 800 MHz; B8 / 900 MHz; B3 / 1800 MHz; B1 / 2100 MHz; B7 / 2600 MHz) max. 23 dBm (LTE), max. 33 dBm (GPRS) FAKRA-Stecker, D-codiert, bordeaux-violett
WAN-A LTE-450 (Fallback GPRS)	Frequenzbereich Ausgangsleistung Anschluss	LTE-Modul (B72 / 450 MHz kein Fallback auf GPRS; B28 / 700 MHz; B20 / 800 MHz; B8 / 900 MHz; B3 / 1800 MHz; B1 / 2100 MHz) max. 24 dBm (LTE), max. 33 dBm (GPRS) FAKRA-Stecker, D-codiert, bordeaux-violett
WAN-1 Ethernet	Ethernet Anschluss	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i) 8P8C-Buchse (RJ45)
Sicherheit/EMV	Sicherheit Störfestigkeit Störaussendung	EN 62368-1, Überspannungskategorie 3 ETSI EN 301 489 ETSI EN 301 489

Temperaturbereich	Festgelegter Betriebsbereich Grenzbereich für den Betrieb Grenzbereich für Lagerung und Transport	−10 °C…+45 °C −25 °C…+55 °C −25 °C…+70 °C
Luftfeuchtigkeit		gemäß EN 50470-1
Umgebungsbedingungen	Mechanisch Elektromagnetisch Vorgesehener Einsatzort	M1 gemäß Messgeräterichtlinie (2014/32/EU) E2 gemäß Messgeräterichtlinie (2014/32/EU) Innenraum gemäß EN IEC 62052-11
Gehäuse	Abmessungen Montage Schutzklasse Schutzart Gehäusematerial Brandeigenschaften	ca. 90 x 72 x 74 mm (H x B x T) auf Hutschienen gemäß IEC 60715 II IP 30 Transparente Gehäuseteile: Polycarbonat, halogenfrei, recycelbar Nicht transparente Gehäuseteile: Polycarbonat glasfaserverstärkt, halogenfrei, recycelbar gemäß EN 62052-31, Kunststoffe gemäß UL94V-0
Gewicht		ca. 200 g

Tabelle 1: Technische Daten CASA 1.0 und CASA 1.1

2.3 Gehäuse- und Anzeigeelemente

Vorderansicht **Seitenansicht von rechts**



1 WAN-A Antennenanschluss
2 LMN-A wireless M-Bus Antennenanschluss
3 Status-LEDs
4 HAN-Schnittstelle
5 [HAN] CLS-Schnittstelle
6 WAN-1 Schnittstelle
7 Anschluss für Betriebsspannung
8 Verriegelung für Mehrwertmodul
9 LMN-1 Schnittstelle
10 Mehrwertmodul (HAN)
11 SIM-Karten Slot

Abbildung 1: Gehäuse- und Anzeigeelemente

2.3.1 LED-Anzeige

Zur optischen Signalisierung von Betriebs- und Fehlerzuständen verfügt der CASA über vier LEDs an der Frontseite.

LED	Bedeutung	Betriebszustand
PWR	Power	**Aus** während der Initialisierung der Firmware. **Blinkt** bei Abschluss der Initialisierung und Start der Dienste. **Leuchtet dauerhaft** sobald die physische Betriebsbereitschaft hergestellt ist. **Heartbeat** (2 x schnell blinken, lange Pause) wenn sich das Gerät im Soft Lock-Down Modus befindet.
TLS	Transport Layer Security	**Blinkt** ab Beginn des Aufbaus des TLS-Kanals. **Leuchtet dauerhaft** wenn die TLS-Verbindung zum GWA mittels eines Wirkzertifikats erfolgt ist. **Blinkt** wenn die TLS-Verbindung zum GWA mittels eines Gütesiegelzertifikats erfolgt ist. **Aus** wenn die Verbindung zum GWA getrennt wurde.

LED	Bedeutung	Betriebszustand
LMC	Local Meter Controller	**Leuchtet dauerhaft** wenn für mindestens einen Zähler im Local Metrological Network (LMN) eine High-Level Data Link Control (HDLC-) Adresse vergeben wurde. **Aus** wenn keine HDLC-Adresse im LMN vergeben wurde. Wenn der CASA entsprechend konfiguriert ist, können zusätzlich folgende Informationen angezeigt werden: **Heartbeat** (2 x schnell blinken, lange Pause), wenn eine Überlastsituation der Stromversorgung für den LMN-Bus erkannt wurde. **Blinkt** (0,5 Sekunden), wenn die Systemzeit ungültig ist (wird nur angezeigt, wenn gleichzeitig mindestens eine HDLC-Adresse am LMN vergeben ist).
wMT	Wireless M-Bus Traffic	**Leuchtet kurz** wenn ein Datensatz über den Wireless M-Bus empfangen wird.
PWR, TLS, LMC, wMT	Hard Lock-Down Modus	**Blinken gemeinsam dauerhaft** wenn sich das Gerät im Hard Lock-Down Modus befindet.

Tabelle 2: LED-Anzeige im Betriebszustand

2.3.2 LEDs Schnittstellen

Die LEDs an den Schnittstellen dienen ausschließlich zur Erkennung einer korrekten Installation durch den Servicetechniker. Zudem unterstützen sie bei der Fehlersuche.

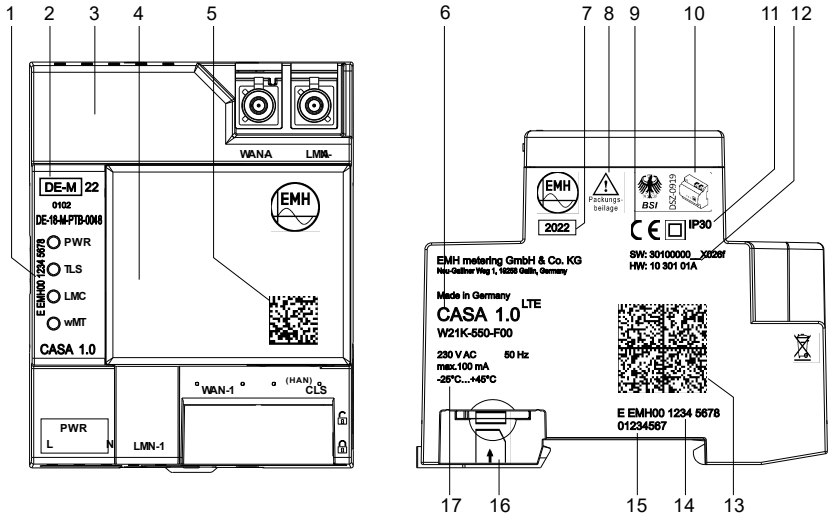
LEDs	Bedeutung	Betriebszustand
An jeweiligen Ethernet-Schnittstellen (HAN, [HAN] CLS, WAN)	Physikalische Ethernet-Anschlüsse	**Leuchtet dauerhaft grün** an der jeweiligen Ethernet-Schnittstelle, sobald die Verbindung zu einem Ethernet-Gerät (z. B. Switch, Router) erkannt wird. **Blinkt gelb** an der jeweiligen Ethernet-Schnittstelle bei Empfang oder Versand von Datenpaketen über die physikalische Ethernet-Verbindung.

Tabelle 3: LEDs Schnittstellen

Die LEDs müssen für den Letztverbraucher nicht zwingend sichtbar sein. Gegebenenfalls sind einige verdeckt.

2.4 Beschriftung des Gerätes – CASA 1.0

Vorderansicht **Seitenansicht von rechts**



1 Herstellerübergreifende Identifikationsnummer (HÜID)
2 Konformitätskennzeichnung
3 Platz für technische Zusatzinformation des Kunden
4 Platz für Eigentumsbeschriftung
5 DataMatrix-Code des Eigentümers
6 Typbezeichnung und Typenschlüssel
7 Baujahr
8 Hinweis auf Packungsbeilage
9 CE-Kennzeichnung
10 BSI Zulassungszeichen
11 Schutzart und Schutzklasse
12 Softwareversion und Hardwareversion
13 DataMatrix-Code (relevante Produktspezifikationen)
14 Herstellerübergreifende Identifikationsnummer (HÜID)
15 Seriennummer des Sicherheitssiegels
16 Abbildung zur Installation der SIM-Karte
17 Spannung, Frequenz, Strom, Betriebstemperatur

Abbildung 2: Beschriftung CASA 1.0

Software-Versionsnummer

Die auf dem Schild angegebene Versionsnummer bezieht sich auf den Zeitpunkt der Herstellung des Gerätes.

Hardware-Versionsnummer

Die Versionsnummer beschreibt in den ersten fünf Stellen den Hardware-Stand des zertifizierungsrelevanten Teils des CASA (im abgebildeten Beispiel „10 301“).

Die letzten drei Stellen der Versionsnummer dokumentieren Bauteile des CASA, die nicht Bestandteil der Zertifizierung nach Common Criteria sind (im abgebildeten Beispiel „01A“).

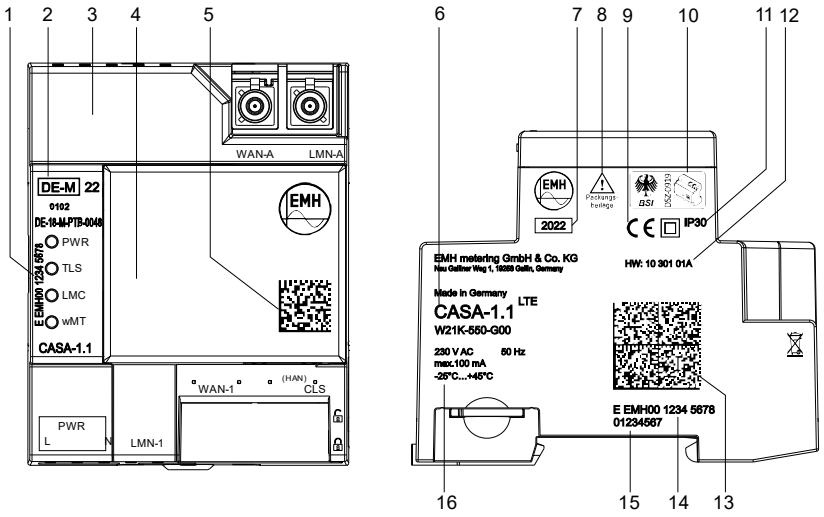
Mögliche Hardwareversionen bei Verwendung von funktionsgleichen Alternativ-Bauteilen:

- 10 301 xxx
- 10 302 xxx
- 10 303 xxx
- 10 304 xxx

2.5 Beschriftung des Gerätes – CASA 1.1

Zusätzlich zu der hier abgebildeten Beschriftung des CASA 1.1 existiert eine alternative Beschriftung. Diese ist auf der nächsten Seite abgebildet.

Vorderansicht **Seitenansicht von rechts**



1 Herstellerübergreifende Identifikationsnummer (HÜID)
2 Konformitätskennzeichnung
3 Platz für technische Zusatzinformation des Kunden
4 Platz für Eigentumsbeschriftung
5 DataMatrix-Code des Eigentümers
6 Typbezeichnung und Typenschlüssel
7 Baujahr
8 Hinweis auf Packungsbeilage
9 CE-Kennzeichnung
10 BSI Zulassungszeichen
11 Schutzart und Schutzklasse
12 Hardwareversion
13 DataMatrix-Code (relevante Produktspezifikationen)
14 Herstellerübergreifende Identifikationsnummer (HÜID)
15 Seriennummer des Sicherheitssiegels
16 Spannung, Frequenz, Strom, Betriebstemperatur

Abbildung 3: Beschriftung CASA 1.1

Hardware-Versionsnummer

Die auf dem Schild angegebene Versionsnummer beschreibt in den ersten fünf Stellen den Hardware-Stand des zertifizierungsrelevanten Teils des CASA (im abgebildeten Beispiel „11 301“).

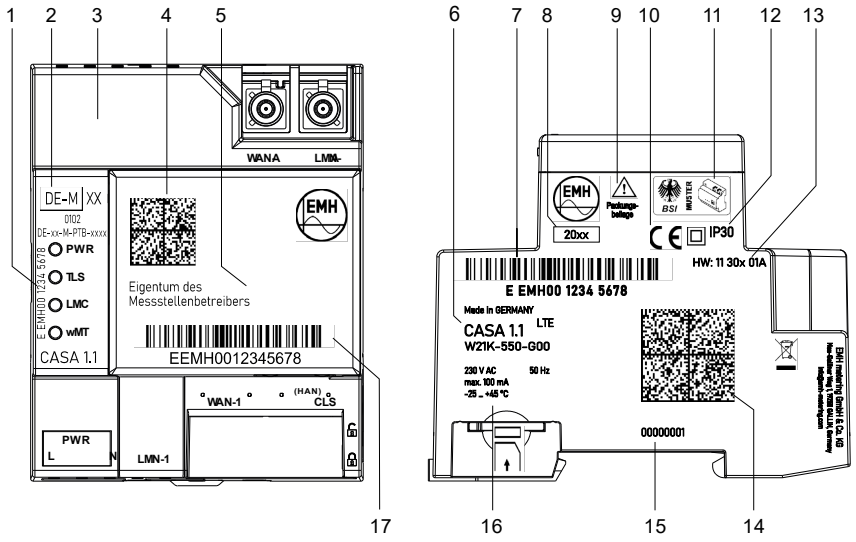
Die letzten drei Stellen der Versionsnummer dokumentieren Bauteile des CASA, die nicht Bestandteil der Zertifizierung nach Common Criteria sind (im abgebildeten Beispiel „01A“).

Mögliche Hardwareversionen bei Verwendung von funktionsgleichen Alternativ-Bauteilen:

- 11 301 xxx
- 11 302 xxx
- 11 501 xxx
- 11 502 xxx

Alternative Beschriftung des Gerätes – CASA 1.1

Vorderansicht **Seitenansicht von rechts**



1 Herstellerübergreifende Identifikationsnummer (HÜID)
2 Konformitätskennzeichnung
3 Platz für technische Zusatzinformation des Kunden
4 DataMatrix-Code des Eigentümers
5 Platz für Eigentumsbeschriftung
6 Typbezeichnung und Typenschlüssel
7 Herstellerübergreifende Identifikationsnummer (HÜID)
8 Baujahr
9 Hinweis auf Packungsbeilage
10 CE-Kennzeichnung
11 BSI Zulassungszeichen
12 Schutzart und Schutzklasse
13 Hardwareversion
14 DataMatrix-Code (relevante Produktspezifikationen)
15 Seriennummer des Sicherheitssiegels
16 Spannung, Frequenz, Strom, Betriebstemperatur
17 Herstellerübergreifende Identifikationsnummer (HÜID)

Abbildung 4: Alternative Beschriftung CASA 1.1

Hardware-Versionsnummer

Die auf dem Schild angegebene Versionsnummer beschreibt in den ersten fünf Stellen den Hardware-Stand des zertifizierungsrelevanten Teils des CASA (im abgebildeten Beispiel „11 301“).

Die letzten drei Stellen der Versionsnummer dokumentieren Bauteile des CASA, die nicht Bestandteil der Zertifizierung nach Common Criteria sind (im abgebildeten Beispiel „01A“).

Mögliche Hardwareversionen bei Verwendung von funktionsgleichen Alternativ-Bauteilen:

- 11 301 xxx
- 11 302 xxx
- 11 501 xxx
- 11 502 xxx

2.6 CASA mit Mehrwertmodul

Das Mehrwertmodul mit seiner Funktion als HAN-Schnittstelle ermöglicht dem Servicetechniker und dem Letztverbraucher einen Zugang zur HAN-Schnittstelle.

Die beim CASA 1.0 und beim CASA 1.1 zum Einsatz kommenden Mehrwertmodule sind baugleich.

Die nachfolgende Abbildung zeigt den CASA mit Mehrwertmodul im betriebsfähigen Zustand.

Abbildung 5: Gehäuse mit Mehrwertmodul

2.7 Kommunikationsschnittstellen

Nachfolgend werden die unterschiedlichen Schnittstellen des CASA beschrieben.

2.7.1 LMN-Schnittstellen

Im Local Metrological Network (LMN) übertragen die angebundenen Zähler für unterschiedliche Medien (Strom, Gas, Wasser, Wärme) ihre Messdaten an den CASA. Die Zähler können einem oder mehreren Letztverbrauchern zugeordnet sein.

Zur Anbindung an das LMN stellt der CASA zwei physikalische Schnittstellen bereit:

- LMN-1 – RS485 ausgeführt als RJ12-Buchse
- LMN-A – wM-Bus ausgeführt als FAKRA-Buchse

2.7.2 HAN-Schnittstelle

Das Home Area Network (HAN) bietet dem Letztverbraucher Zugriff auf den CASA. Der Letztverbraucher kann die ihm zugeordneten Informationen abrufen.

Die HAN-Schnittstelle ist physikalisch mit einer RJ45-Buchse realisiert.

2.7.3 [HAN] CLS-Schnittstelle

Die [HAN] CLS-Schnittstelle dient zur Kommunikation des CASA mit Geräten des Letztverbrauchers mittels CLS (Controllable Local Systems). CLS dient dazu, Erzeuger und Verbraucher von z. B. Energie flexibel in das jeweilige Netz zu integrieren. Bei den CLS-Geräten des Letztverbrauchers kann es sich z. B. um Steuerboxen, Kraft-Wärme-Kopplungs-Anlagen oder Photovoltaik-Anlagen handeln.

Die Steuerung dieser Kommunikation erfolgt durch externe Marktteilnehmer im WAN.

Der Aufbau einer Verbindung zwischen einem externen Marktteilnehmer (EMT) und dem CASA kann nicht direkt vom EMT ausgelöst werden. Dies geschieht über den Gateway-Administrator, welcher den Verbindungsaufbau im CASA initiiert.

Ein CLS-Gerät (z. B. Steuerbox oder HEMS) hingegen kann den EMT direkt über den CASA ansprechen, weil die Zertifikate des CLS-Gerätes zuvor vom Gateway-Administrator in den CASA eingespielt wurden.

2.7.4 WAN-Schnittstellen

Im Wide Area Network (WAN) kommuniziert der CASA mit dem Gateway-Administrator sowie mit externen Marktteilnehmern.

Zur Anbindung an das WAN stellt der CASA zwei verschiedene physikalische Schnittstellen bereit:

- WAN-A (Funkschnittstelle zur Nutzung der Netzstandards LTE und GPRS)
- WAN-1 (Ethernet-Verbindung, ausgeführt als RJ45-Buchse)

Ein einwandfreier Betrieb des CASA über die WAN-A Schnittstelle setzt eine ausreichend gute Funkverbindung voraus.

2.8 Fehlerzustände

Der CASA kennt zwei unterschiedliche Fehlerzustände:

- Soft Lock-Down Modus
- Hard Lock-Down Modus

Diese werden in den nächsten Abschnitten beschrieben.

2.8.1 Soft Lock-Down Modus

Der Soft Lock-Down Modus wird u. a. ausgelöst, wenn eines der folgenden Ereignisse eintritt:

- Weniger als 10 % des Systemspeichers stehen zur Verfügung.
- Der Selbsttest wurde mit einem kritischen Fehler beendet.
- Das System erkennt eine Veränderung an der Hardware.
- Das System kann über einen Zeitraum von 48 Stunden keine Zeitsynchronisation erfolgreich durchführen.
- Die Zeitabweichung bei Synchronisation beträgt mehr als 3 % der Abrechnungsperiode (entspricht 27 Sekunden).

Weitere Ereignisse, die zur Auslösung des Soft Lock-Down Modus führen, sind in Kapitel 6.3 / Seite 46 aufgeführt.

Im Soft Lock-Down Modus werden keine weiteren Zählerdaten eingesammelt, tarifiert oder versendet. Zudem hat der Letztverbraucher keinen weiteren Zugriff auf die Daten.

Im Soft Lock-Down Modus baut der CASA automatisch eine Verbindung zum Gateway-Administrator auf, womit dieser über den Fehlerzustand informiert wird.

2.8.2 Hard Lock-Down Modus

Der Hard Lock-Down Modus wird ausgelöst, wenn beide Ereignisse eintreten:

1. Der CASA stellt im laufenden Betrieb einen Integritätsfehler der Firmware fest, woraufhin der Gateway-Administrator eine entsprechende Information erhält und das Gerät einen Neustart ausführt.
2. Während des anschließenden Systemhochlaufs tritt der Fehler im Rahmen der Integritätstests erneut auf.

Im Hard Lock-Down Modus ist der CASA dauerhaft an keiner Schnittstelle und durch keinen Akteur erreichbar und muss ersetzt werden.

2.9 Funktionen

Der CASA kann die Zählerstände von mehreren angeschlossenen Zählern für unterschiedliche Medien erfassen, wobei jeder Zähler über seine Geräte-ID eindeutig identifizierbar und adressierbar ist.

Die Verarbeitung der erfassten Messwerte verfolgt dabei mehrere Zwecke:

- Tarifierung von Verbrauchs- und Einspeisemengen
- Erhebung von Netzzustandsdaten
- Bilanzierung von Energienetzen durch Netzbetreiber

Im nächsten Abschnitt werden die vom CASA unterstützten Anwendungsfälle beschrieben.

2.9.1 Tarifanwendungsfälle

Bei jedem der hier beschriebenen Tarifanwendungsfälle (TAF) erhält der externe Marktteilnehmer (EMT) die vom CASA erfasste Messwertliste.

Die Zähler werden über ihre Identifikationsnummer, die zu erfassenden Messgrößen werden über die entsprechenden OBIS-Kennzahlen ausgewählt. Abrechnungsrelevante Daten werden vom CASA vor der Inhaltsverschlüsselung mit einer zusätzlichen Signatur versehen.

Der Versand der Messwertliste an die berechtigten Marktteilnehmer erfolgt zu einem frei konfigurierbaren Zeitpunkt.

Der Gültigkeitszeitraum legt fest, zu welchem Zeitpunkt das Regelwerk für einen Anwendungsfall aktiviert bzw. deaktiviert wird.

TAF1 – Datensparsame Tarife

Datensparsame Tarife werden für Verbrauchsabrechnungen herangezogen bei denen verhindert werden soll, dass auf Basis der vom CASA versandten Messwerte Aussagen über das Verbrauchsverhalten des Letztverbrauchers getroffen werden können.

Dabei wird nur eine Tarifstufe betrachtet. Zu diesem Zweck übermittelt der CASA von einem oder mehreren angeschlossenen Zählern jeweils nur einen Zählerstand pro Abrechnungszeitraum an den autorisierten externen Marktteilnehmer (EMT). Der Abrechnungszeitraum muss sich dabei über mindestens 1 Monat erstrecken und ist vom Gateway-Administrator entsprechend zu konfigurieren.

TAF2 – Zeitvariable Tarife

Bei diesem Anwendungsfall stellt der Lieferant dem Letztverbraucher variierende Preise für die in unterschiedlichen Zeiträumen registrierten Energiemengen in Rechnung.

Hierzu werden im CASA mehrere Tarifstufen definiert, die jeweils an eine Zeitbedingung geknüpft sind. Die Zeitbedingungen wiederum werden über Tarifschaltzeitpunkte definiert, wobei zu jedem Zeitpunkt jeweils nur eine Tarifstufe aktiv ist.

Zu einem Tarifschaltzeitpunkt erfasst der CASA die Zählerstände von einem oder mehreren Zählern. Der CASA erzeugt einen Eintrag in der Messwertliste und fügt die zwischen den beiden letzten Tarifschaltzeitpunkten angefallene Energiemenge der zuletzt gültigen Tarifstufe hinzu.

TAF6 – Abruf von Messwerten im Bedarfsfall

Dieser Anwendungsfall erlaubt den Abruf von Messwerten in besonderen, begründeten Fällen.

Beispiele hierfür sind:

- Ein- oder Auszug eines Letztverbrauchers
- Wechsel des Lieferanten
- Wechsel in den Grundversorgungstarif

Damit rückwirkende Ablesungen zu einem bestimmten Stichtag möglich sind, hält der CASA tagesgenaue Zählerstände für jeden angeschlossenen Zähler vor. Zu diesem Zweck erfasst der CASA täglich zum Beginn des

abrechnungstechnischen Kalendertages den aktuellen Zählerstand und erzeugt einen Eintrag in der Messwertliste. Messwerte, die älter als 6 Wochen sind, werden automatisch aus der Messwertliste gelöscht.

Im begründeten Ausnahmefall werden die Daten im Auftrag eines externen Marktteilnehmers durch den Gateway-Administrator ausgelesen und zu einem Stichtag an den externen Marktteilnehmer weitergeleitet.

TAF7 – Zählerstandsgangmessung

Dieser Anwendungsfall erlaubt die Erfassung und den Versand von Zählerstandsgängen. Dadurch ist unter anderem die zentrale Tarifierung außerhalb des CASA möglich. Der CASA erfasst die Zählerstände im Takt der Registrierperiode und erzeugt einen Eintrag in der zugehörigen Messwertliste.

TAF9 – Bereitstellung der Ist-Einspeisung einer Erzeugungsanlage

§ Die Daten, die bei diesem Anwendungsfall erhoben werden, sind nicht abrechnungsrelevant und werden pseudonymisiert verschickt. Bei entsprechender Zweckbindung im Rahmen einer vertraglichen Regelung kann die Pseudonymisierung deaktiviert werden.

Dieser Anwendungsfall erlaubt die Erfassung und den Versand der Ist-Einspeiseleistung an Anlagen nach dem EEG (Erneuerbare-Energien-Gesetz) und dem KWKG (Kraft-Wärme-Kopplungsgesetz).

Neben dem periodischen Versand per Konfiguration unterstützt der CASA die folgenden Ereignisse zur Auslösung des Datenversands:

- Versand im Bedarfsfall auf Veranlassung durch den Gateway-Administrator
- Versand bei Schwellenwertüber- oder Unterschreitung

Als Eingangsgrößen für den TAF9 können die Momentanwerte der Gesamt-Einspeisewirkleistung (P_{ges}) und die Momentanwerte der Einspeisewirkleistung einzelner Phasen (P_{L1}, P_{L2}, P_{L3}) konfiguriert werden. Aus diesen Messgrößen können zusätzlich aggregierte Werte gebildet werden (Maximum-, Minimum- und Mittelwertbildung).

TAF10 – Abruf von Netzzustandsdaten

§ Die Daten, die bei diesem Anwendungsfall erhoben werden, sind nicht verrechnungsrelevant und werden pseudonymisiert verschickt. Bei entsprechender Zweckbindung im Rahmen einer vertraglichen Regelung kann die Pseudonymisierung deaktiviert werden.

Im CASA können Netzzustandsdaten bzw. Statusinformationen der angeschlossenen Zähler bereitgestellt werden. Dies ermöglicht es Netzbetreibern, den Zustand ihrer Netze zu beurteilen.

Diese Daten können periodisch oder bei Eintritt bestimmter Ereignisse an die berechtigten Marktteilnehmer versendet werden.

Neben dem periodischen Versand per Konfiguration unterstützt der CASA die folgenden Ereignisse zur Auslösung des Datenversands:

- Versand im Bedarfsfall auf Veranlassung durch den Gateway-Administrator
- Versand bei Schwellenwertüber- oder Unterschreitung

Für die Überwachung der Netzzustandsdaten stehen für diesen TAF folgende Eingangsgrößen zur Verfügung:

- Momentanwert der Gesamtwirkleistung P_{ges}
- Momentanwert der Phasenwirkleistung (P_{L1}, P_{L2}, P_{L3})
- Frequenz
- Phasenwinkel zwischen den Spannungen verschiedener Phasen: U_{L2} zu U_{L1} und U_{L3} zu U_{L1}
- Phasenwinkel zwischen Strom und Spannung derselben Phase, bspw. I_{L1} zu U_{L1}
- Phasenstrom (I_{L1}, I_{L2}, I_{L3})
- Phasenspannung (U_{L1}, U_{L2}, U_{L3})

Aus diesen Messgrößen können zusätzlich aggregierte Werte gebildet werden (Maximum-, Minimum- und Mittelwertbildung).

TAF14 – Hochfrequente Messwertbereitstellung für Mehrwertdienste

§ Die Daten, die bei diesem Anwendungsfall erhoben werden, sind nicht abrechnungsrelevant und werden pseudonymisiert verschickt. Bei entsprechender Zweckbindung im Rahmen einer vertraglichen Regelung kann die Pseudonymisierung deaktiviert werden.

Dieser Anwendungsfall erlaubt die hochfrequente Auslesung und Bereitstellung von Messwerten. Die kürzeste Abtastperiode beträgt 60 Sekunden.

Neben dem periodischen Versand per Konfiguration unterstützt der CASA die folgenden Ereignisse zur Auslösung des Datenversands:

- Ad-hoc-Versand (jeder eingehende Messwert wird direkt versendet)
- Versand bei Schwellenwertüber- oder Unterschreitung

Anders als bei TAF9 und TAF10 wird hier bei einer Schwellenwertüber- oder Unterschreitung nicht nur der aktuelle Messwert versendet, sondern die komplette Liste aller bis dahin nicht versandten Messwerte.

Für den TAF14 stehen folgende Eingangsgrößen zur Verfügung:

- Gesamtwirkenergie in Richtung A+
- Phasenwirkenergie in Richtung A+ für $L_{(1-3)}$
- Gesamtwirkenergie in Richtung A−
- Phasenwirkenergie in Richtung A− für $L_{(1-3)}$
- Blindenergie in Richtung $R_{(1-4)}$
- Momentanwert der Gesamtwirkleistung P_{ges}
- Momentanwert der Phasenwirkleistung (P_{L1}, P_{L2}, P_{L3})

2.9.2 Logbücher

Der CASA protokolliert seine Aktionen in drei unterschiedlichen Logbüchern, welche in den nachfolgenden Kapiteln beschrieben werden:

- Letztverbraucher-Log
- System-Log
- Eich-Log

Folgende Tabelle gibt Aufschluss über die Zugriffsmöglichkeiten:

Log	Zugriff	Schnittstelle
Letztverbraucher-Log	lesender Zugriff durch den Letztverbraucher	HAN- und [HAN] CLS-Schnittstelle
System-Log	lesender Zugriff durch den Gateway-Administrator	WAN-Schnittstelle
	lesender Zugriff durch den Servicetechniker	HAN-Schnittstelle
Eich-Log	lesender Zugriff durch den Gateway-Administrator	WAN-Schnittstelle

Tabelle 4: Zugriffsmöglichkeiten auf Logbücher

Jeder Logbucheintrag setzt sich aus den folgenden Informationen zusammen:

- Zeitstempel
- Eindeutige Logbuchmeldung-Identifikationsnummer, die das eingetretene Ereignis beschreibt
- Digitale Signatur (nur für das Eich-Log)

2.9.2.1 Letztverbraucher-Log

Ein Letztverbraucher hat Zugriff auf das Letztverbraucher-Log, wenn er die entsprechenden Zugangsdaten für die Authentifizierung von seinem Messstellenbetreiber erhalten hat.

Über das Letztverbraucher-Log ist nachzuverfolgen, wer, wann, welche Daten erhalten hat, oder ob benutzerbezogene Daten (z. B. Profile) geändert bzw. hinzugefügt oder entfernt wurden. Zur Wahrung der Vertraulichkeit der personenbezogenen Protokolldaten ist ausschließlich dem Letztverbraucher der Zugriff auf das Letztverbraucher-Log gestattet. Jeder Letztverbraucher hat sein eigenes Letztverbraucher-Log.

Die Informationen des Letztverbraucher-Logs werden vom CASA derart aufbereitet, dass der autorisierte Letztverbraucher sie mit einem Webbrowser an der HAN- oder [HAN] CLS-Schnittstelle ohne weitere Hilfsmittel lesen kann.

Die im Letztverbraucher-Log aufgezeichneten Ereignisse können weder gelöscht noch bearbeitet werden. Dies gilt für sämtliche Rollen bzw. Akteure.

Die Speicherdauer kann durch den Gateway-Administrator konfiguriert werden, beträgt jedoch mindestens 15 Monate.

Eine Liste der im Letztverbraucher-Log protokollierten Ereignisse finden Sie in Kapitel 6.2 / Seite 42.

2.9.2.2 System-Log

Das System-Log dient dazu, den Gateway-Administrator und den autorisierten Servicetechniker über den Systemstatus des CASA zu informieren.

Im System-Log protokolliert der CASA jedes wichtige Ereignis (z. B. Fehlermeldungen, Ausfall der WAN-Verbindung, sicherheitsrelevante Ereignisse, Aktivitäten des Gateway-Administrators, etc.). Die Informationen dienen ausschließlich dazu, den momentanen Status des CASA zu erkennen und eventuelle Fehlerquellen oder Störungen zu identifizieren Im System-Log werden keine datenschutzrelevanten Informationen (z. B. Zähler-Daten oder Messwerte) gespeichert.

2.9.2.3 Eich-Log

Im Eich-Log werden rechtlich relevante Ereignisse (z. B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) beständig und nachvollziehbar gespeichert. Außerdem erfolgt die Registrierung von Änderungen an rechtlich relevanten Parametern (z. B. Zeitsprünge bei der Uhrzeitsynchronisation oder Änderungen der Tarifprofile).

Jeder Eintrag im Eich-Log ist durch eine digitale Signatur mit dem privaten Signaturschlüssel des CASA versehen. Damit ist die Integrität und Authentizität des Eich-Log sichergestellt.

2.10 Firmware-Update

Der CASA ist ein IT-System, welches einer stetigen Weiterentwicklung unterliegt. Alle Updates der Firmware werden durch kryptografische Signaturfunktionen vor Manipulation und Übertragungsfehlern geschützt.

Das Firmware-Update wird durch den Gateway-Administrator durchgeführt.

Die Applikationsdaten im CASA (wie z. B. Messwertlisten, Zählerprofile, Auswertungsprofile, Kommunikationsprofile) werden durch ein Firmware-Update weder verändert noch gelöscht.

3 Prüfung der Integrität des CASA

Die Integrität des CASA muss vor der Montage und Inbetriebnahme durch den Servicetechniker überprüft werden. Dazu werden die äußeren Sicherheitsmerkmale am Gerät überprüft.

Das Sicherheitssiegel muss auf seine Unversehrtheit überprüft werden.
Die Darstellungen für unbeschädigte Siegel und beschädigte Siegel finden Sie in Kapitel 3.1.2. / Seite 26 und in Kapitel 3.1.3 / Seite 26.

Falls Beschädigungen am Gehäuse oder am Sicherheitssiegel des CASA festgestellt werden, darf das Gerät nicht verwendet werden!

In diesem Fall muss der Messstellenbetreiber informiert werden.

3.1 CASA Sicherheitssiegel

In der nachfolgenden Abbildung ist die vertiefte Fläche am Gerät dargestellt, auf welche das Siegel aufgebracht wird.

Die korrekt zusammengeführten Gehäusekanten sind zu erkennen, welche im Herstellungsprozess mit dem Sicherheitssiegel beklebt werden. Auf diese Weise wird das nicht autorisierte Öffnen des Gehäuses erkennbar gemacht.

1 Vertiefung für Sicherheitssiegel

Abbildung 6: Position des Sicherheitssiegels (linke Seite des CASA, gegen den Uhrzeigersinn gedreht)

3.1.1 EMH Sicherheitssiegel

Die nachfolgende Abbildung zeigt die Gesamtansicht des EMH Sicherheitssiegels sowie seine Abmessungen bei Beleuchtung mit Tageslicht.

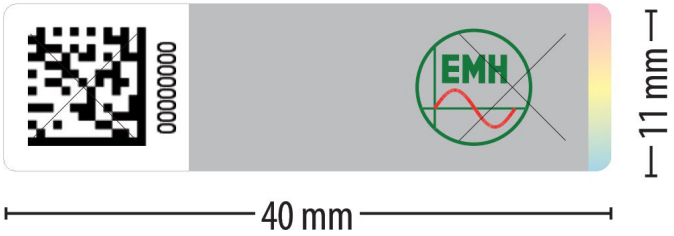


Abbildung 7: EMH Sicherheitssiegel – Beleuchtung mit Tageslicht

Bei Beleuchtung mit UV-Licht wird das gelb-grünlich leuchtende Sicherheitsmerkmal des Siegels erkennbar.

Abbildung 8: EMH Sicherheitssiegel – Beleuchtung mit UV-Licht

Die nachfolgenden Abbildungen zeigen weitere Sicherheitsmerkmale des EMH Sicherheitssiegels.

Jedes Siegel ist mit einer eindeutigen Seriennummer gekennzeichnet, welche sowohl in lesbarer Form als auch in einem DataMatrix-Code aufgedruckt ist. Zudem ist die Seriennummer im Typenschild des CASA an der Gehäuseseite angegeben.

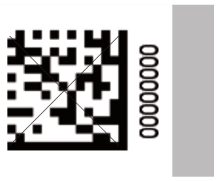


Abbildung 9: EMH Sicherheitssiegel – Seriennummer

Der DataMatrix-Code und das EMH-Logo verfügen beide über eine Sicherheitsstanzung, erkennbar an den zwei schrägen Linien.

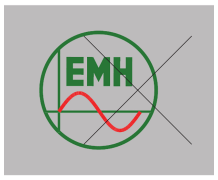


Abbildung 10: EMH Sicherheitssiegel – Sicherheitsstanzung

Das optische Echtheitsmerkmal des Siegels zeigt bei bestimmtem Lichteinfall einen Verlauf des gesamten sichtbaren Farbspektrums.

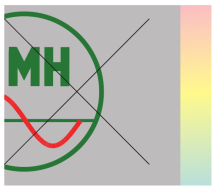


Abbildung 11: EMH Sicherheitssiegel – Optisches Echtheitsmerkmal

3.1.2 Unbeschädigtes Sicherheitssiegel

Die nachfolgende Tabelle zeigt Beispiele für unbeschädigte, korrekt positionierte Sicherheitssiegel.

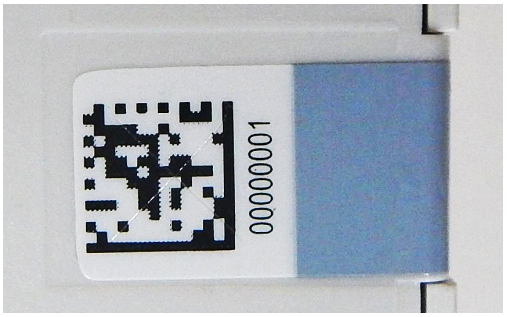
Unbeschädigtes Siegel	Beschreibung	Verwendung
	korrektes Siegel	✓
	korrektes Siegel	✓
	korrektes Siegel	✓

Tabelle 5: Unbeschädigtes Siegel – Beispiele

3.1.3 Beschädigtes Sicherheitssiegel

In der folgenden Tabelle sind einige Beispiele für beschädigte Sicherheitssiegel dargestellt.
Zur Vorgehensweise bei beschädigtem Sicherheitssiegel siehe erster Abschnitt in Kapitel 3 / Seite 24.

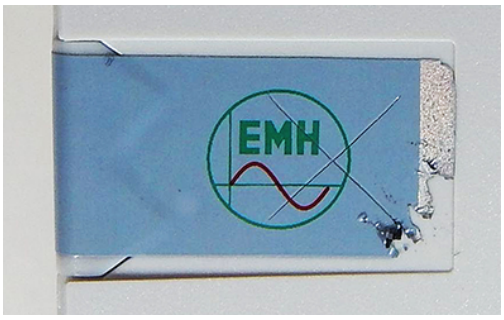
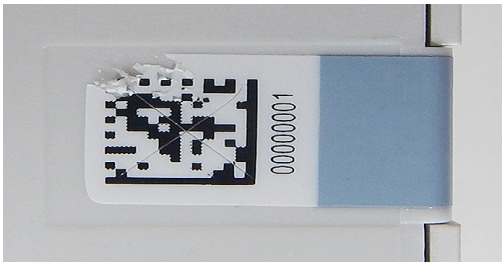
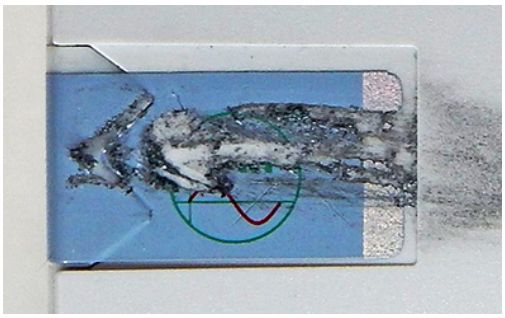
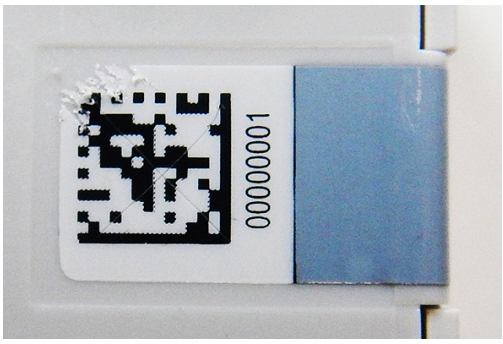
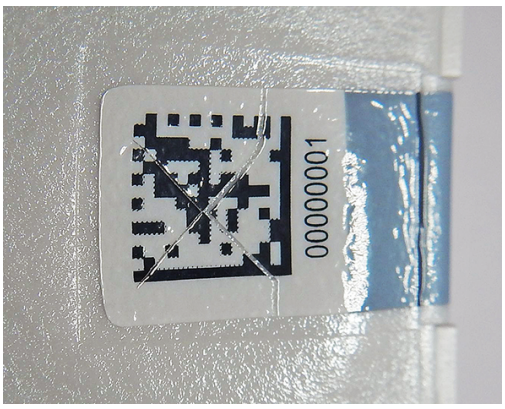
Beschädigtes Siegel	Beschreibung	Verwendung
	zerstörtes Siegel nach mechanischem Manipulations-versuch	✗
	zerstörtes Siegel nach mechanischem Manipulations-versuch	✗
	zerstörtes Siegel nach Manipulations-versuch mit chemischen Lösungsmitteln	✗
	zerstörtes Siegel nach mechanischem Manipulations-versuch mit Kälteeinwirkung	✗
	zerstörtes Siegel nach mechanischem Manipulations-versuch mit Wärmeeinwirkung	✗

Tabelle 6: Beschädigtes Siegel – Beispiele

4 Prozessuale Sicherheit

Das SMGW ist die zentrale Schnittstelle eines iMSys.

Daraus ergeben sich spezielle Sicherheitsanforderungen sowohl an das Gerät als auch an die Rollen der beteiligten Akteure und deren Prozesse.

Für die Realisierung der sicheren Lieferkette wird neben einer sicheren IT-Infrastruktur und definierten Prozessen auch vertrauenswürdiges, verantwortliches und geschultes Personal benötigt.

4.1 Internes Sicherheitskonzept des CASA

4.1.1 Softwaresicherheitskonzept

Die Software des CASA beinhaltet zahlreiche Mechanismen zur Absicherung des Systems:

- gegen zufällige und unbeabsichtigte Informationsveränderungen
- gegen gezielte Manipulationen
- zur Vermeidung von Bedienfehlern durch Gateway-Administratoren, Servicetechniker oder Letztverbraucher

Gemäß Schutzprofil BSI-CC-PP-0073 und Technischer Richtlinie BSI-TR-03109-1 basiert das Schutzkonzept auf asymmetrischer Kryptografie mit privaten und öffentlichen Schlüsseln sowie symmetrischer Kryptografie mittels AES-Algorithmus.

Öffentlichen Schlüsseln wird durch ihre Mitgliedschaft in einer Public Key Infrastructure (PKI) Vertrauen in Form von Zertifikaten ausgesprochen. Die bei der Kommunikation mit dem Gateway-Administrator verwendeten Zertifikate sind auf einen Vertrauensanker in der Root-CA (Root Certificate Authority) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zurückzuführen.

4.1.2 Schutz der gespeicherten Messwerte gegen Verfälschung

Es ist nicht möglich, die im CASA gespeicherten Messwerte durch Zugriff über eine der Geräteschnittstellen zu verändern. Dies gilt für alle Rollen der unterschiedlichen Akteure, siehe hierzu Kapitel 4.2.1 / Seite 30.

Abrechnungsrelevante Daten sind zudem mit einer digitalen Signatur versehen, die eine unbemerkte Verfälschung der Daten ausschließt.

4.1.3 Schutz des Programmcodes

Der CASA führt eine automatische, zyklische Prüfung (Selbsttest) der rechtlich relevanten Software im Langzeitspeicher durch. Diese Prüfung kann zudem durch den Gateway-Administrator, den Servicetechniker oder den Letztverbraucher durchgeführt werden.
Im Zuge dieser Prüfung werden die Signaturen der installierten Software verifiziert. Dadurch kann eine zufällige Informationsverfälschung oder Manipulation des Langzeitspeichers zuverlässig erkannt werden.

4.1.4 Schutz von übertragenen und gespeicherten Daten

Die rechtlich relevante Software fasst die zu einem Messzeitpunkt erfassten Informationen eines Zählers zu einem Zählerdatensatz zusammen, welcher bei verrechnungsrelevanten Daten digital signiert wird.

Die digitale Signatur wird vor der Langzeitspeicherung mit dem Datensatz verknüpft. Somit können von einem empfangenden Gerät mittels Signaturprüfung eventuelle Verfälschungen des Datensatzes erkannt werden. Dies gelingt unabhängig davon, ob die Verfälschung im Datenspeicher oder während der Datenfernübertragung erfolgt ist.

Das Signaturzertifikat des CASA, das zur Prüfung der Signaturen in den Datensätzen erforderlich ist, wird vorab in den CASA eingespielt und den entsprechenden Messstellenbetreibern verfälschungssicher zur Verfügung gestellt. Der Letztverbraucher kann dieses Zertifikat über die Letztverbraucherschnittstelle (HAN) auslesen.

Der CASA führt eine automatische, zyklische Prüfung der Messwerte (Selbsttest) im Langzeitspeicher durch. Diese Prüfung kann zudem durch den Gateway-Administrator, den Servicetechniker oder den Letztverbraucher durchgeführt werden.
Dadurch kann eine zufällige Informationsverfälschung oder Manipulation des Langzeitspeichers zuverlässig erkannt werden.

4.1.5 Fehlerereignisse der Zählerdaten

Die folgenden Fehlerereignisse werden vom CASA erkannt:

- dauerhaft ausbleibender Empfang von Zählerdaten
- wiederholt auftretende Transportfehler
- die Schnittstelle zum Empfang von Zählerdaten ist nicht ansprechbar oder nicht vorhanden

In diesen Fällen wird vom CASA eine Fehlermeldung generiert und an den Gateway-Administrator gesendet.

4.1.6 Kommunikationsprotokolle und Profile

Zur Sicherung der Kommunikationswege von und zum CASA kommt das Protokoll TLS (Transport Layer Security) in der Version 1.2 zur Anwendung.

Beim Aufbau jeder TLS-Verbindung wird die Authentizität der Kommunikationspartner anhand wechselseitig ausgetauschter Zertifikate geprüft.

4.1.7 Inhaltsdatensicherung und Signaturbildung

Die für externe Marktteilnehmer bestimmten Netzzustands- und Verrechnungsdaten werden vom CASA (ggf. über den Gateway-Administrator) an die externen Marktteilnehmer übertragen.
Der Dateninhalt ist dabei

- verschlüsselt,
- über Message Authentication Code (MAC) gesichert und
- für die Empfänger gekennzeichnet und signiert.

Darüber hinaus verschlüsselt der CASA seine lokalen Daten während der Speicherung in einem persistenten Speicher.

4.1.8 Pseudonymisierung von Daten

Die Messwerte, die im Rahmen eines TAF9 oder TAF10 erfasst werden, können vor der Übertragung an den externen Marktteilnehmer oder den Gateway-Administrator pseudonymisiert werden.
Auf diese Weise wird verhindert, dass der Empfänger die Daten einem Letztverbraucher zuordnen kann.

Die Pseudonymisierung von Netzzustandsdaten (TAF10) bei der Übertragung vom CASA an einen externen Marktteilnehmer erfolgt durch folgende Schritte:

- Die Geräte-ID wird durch den CASA aus den Messwerten entfernt und durch ein im Auswertungsprofil hinterlegtes Pseudonym ersetzt.
- Die so aufbereiteten Daten werden anschließend vom CASA für den Empfänger verschlüsselt, signiert und direkt an den externen Marktteilnehmer oder an den Gateway-Administrator übertragen.
- Der Gateway-Administrator prüft die Signatur des CASA und damit die Authentizität der Daten. Anschließend leitet er die Daten nach Entfernung der CASA-Signatur an den Empfänger weiter.
- Der Empfänger entschlüsselt die Daten.

4.2 Organisatorische Hinweise

Die organisatorischen Hinweise umfassen das Rollenkonzept, die Tätigkeitsschwerpunkte bzw. Funktionen der beteiligten Akteure sowie deren Identifizierung und Authentifizierung durch den CASA.

4.2.1 Rollenkonzept

Hier werden die Rollen der verschiedenen Akteure beschrieben.

Gateway-Administrator

Der Gateway-Administrator nimmt den CASA in Betrieb.
Er

- konfiguriert, überwacht und steuert das Gerät,
- erstellt und administriert Tarifprofile,
- führt bei Bedarf die Aktualisierung der Software des CASA durch.

Für jeden einzelnen CASA gibt es nur einen Gateway-Administrator.

Servicetechniker

Der Servicetechniker kann die mit HAN und [HAN] CLS bezeichneten Anschlüsse nutzen, um z. B. das System-Log zur Diagnose von Fehlersituationen einzusehen und grundlegende Systemeinstellungen vorzunehmen.

Letztverbraucher

Letztverbraucher sind natürliche oder juristische Personen, die Energie für den eigenen Verbrauch oder den Betrieb von Ladepunkten zur Versorgung von Elektrofahrzeugen beziehen bzw. einspeisen.

Der Letztverbraucher

- ist Eigentümer der im CASA verarbeiteten und gespeicherten Messwerte,.
- hat die Rolle des Anschlussnutzers, ggf. des Anschlussnehmers und des Anlagenbetreibers,
- kann Informationen einsehen, die ihn betreffen (Messwertlisten, Verbrauchs- und/oder Einspeisewerte, Letztverbraucher-Log),
- kann den Selbsttest über das CASA-Benutzerportal ausführen.

Der Letztverbraucher kann keine Daten einsehen, die andere Letztverbraucher betreffen.

Externer Marktteilnehmer

Jeder, mit dem der CASA eine WAN-Kommunikation zum Austausch von Daten aufnehmen kann, wird als externer Marktteilnehmer bezeichnet. Der Gateway-Administrator bildet die Ausnahme, er zählt nicht zu den externen Marktteilnehmern.

Der externe Marktteilnehmer

- ist vertrauenswürdig, autorisiert und wird bei jedem Verbindungsaufbau authentifiziert,
- erhält private oder abrechnungsrelevante Daten,
- darf keine unautorisierten Auswertungen dieser Daten mit Bezug auf den Letztverbraucher durchführen.

Externe Marktteilnehmer haben weder schreibenden Zugriff auf den CASA, noch können sie Daten des CASA aktiv auslesen. Der Versand von Messwerten an den externen Marktteilnehmer geht stets vom CASA aus.

Messstellenbetreiber

Der Messstellenbetreiber ist für die Einrichtung und den Betrieb einer Messstelle verantwortlich.

Er

- nimmt den vom Hersteller gelieferten CASA entgegen,
- beauftragt einen Servicetechniker mit der Montage des Gerätes an der betreffenden Messstelle,
- ist verantwortlich für die ordnungsgemäße Inbetriebnahme und den Betrieb des CASA,
- beauftragt hierzu einen Gateway-Administrator,
- erhält die von den Zählern erzeugten und vom CASA über den Gateway-Administrator weitergeleiteten Messdaten,
- rechnet die erhaltenen Messdaten gegenüber dem Letztverbraucher ab.

Der Messstellenbetreiber hat keinen direkten Zugriff auf den CASA. Er bedient sich stattdessen des von ihm beauftragten Servicetechnikers und des Gateway-Administrators.

4.2.2 Identifizierung und Authentifizierung

Jeder berechtigte Nutzer, der mit dem CASA kommuniziert oder Daten vom CASA erhält, wird vor jeder Aktion identifiziert und authentifiziert.

Hierfür erhält der CASA für jeden Nutzer die folgenden Merkmale:

- Identität des Nutzers
- Status der Identität (authentifiziert oder nicht authentifiziert)
- Verbindungsnetzwerk (WAN, HAN oder LMN)
- Rolle des Nutzers

Der Authentifizierungsprozess erfolgt in der Regel während des TLS-Handshakes beim Aufbau eines TLS-Kanals. Je nach Rolle werden hierzu Client- oder Serverzertifikate ausgetauscht, die anschließend vom CASA mit den im Gerät hinterlegten Zertifikaten verglichen werden (siehe Kapitel 4.1.1 / Seite 28).
Dadurch kann die Gegenstelle genau einem Profil zugeordnet und sowohl authentifiziert als auch identifiziert werden.

Eine Ausnahme bildet dabei der Letztverbraucher, der anstelle eines Client-Zertifikats alternativ auch eine Benutzername/Passwort-Kombination zur Authentifizierung verwenden kann. Dies muss im CASA durch den Gateway-Administrator entsprechend konfiguriert werden.

5 Nutzung des CASA durch den Letztverbraucher

Der CASA bietet dem Letztverbraucher die Möglichkeit, die für ihn bestimmten Mess- und Logdaten zu Informationszwecken darzustellen. Zudem kann der Letztverbraucher einen Selbsttest des CASA auslösen.

Zur Auslesung und Visualisierung der Daten stellt der CASA eine Web-Oberfläche, das CASA-Benutzerportal, zur Verfügung.

Die Zugangsdaten, die Sie als Letztverbraucher für den Zugriff auf Ihre Daten im CASA benötigen, erhalten Sie von Ihrem Messstellenbetreiber.

Bei den Zugangsdaten handelt es sich um:

- HAN IP-Adresse des CASA (anpassbar an Ihr Netzwerk durch den Gateway-Administrator)
- Benutzernamen und Passwort, alternativ TLS-Zertifikat

Das zur Authentifizierung bereitgestellte Zertifikatsmaterial sowie Benutzername und Passwort sind für Dritte unzugänglich aufzubewahren.

Bei fehlerhaften Eingaben werden vom CASA Fehler als HTTP-Statuscodes zurückgemeldet. In diesem Fall korrigieren Sie bitte Ihre Eingabe.

Die Tabelle gibt Aufschluss über die möglichen Statuscodes.

Statuscode	Beschreibung
200 OK	Der Request war erfolgreich.
303 Redirect	Eine Umleitung auf eine andere URI.
400 Bad Request	Fehlendes oder ungültiges HOST-Feld im Header.
401 Unauthorized	Fehlende Authentisierung.
403 Forbidden	Es wurde auf eine Ressource zugegriffen, die einen TLS-Kanal erfordert.
404 Not Found	Zugriff auf eine ungültige URI.
405 Method not allowed	Falsche HTTP Methode auf vorhandene Ressource. Nur GET-Methoden sind zulässig.
422 Unprocessable Entry	Ungültige Query-Parameter.
423 Locked	Zu viele fehlgeschlagene Authentifizierungsversuche. Zugang ist für 5 Minuten gesperrt.
429 Too Many Requests	Zu viele gleichzeitige Verbindungsanfragen. Zugang ist vorübergehend gesperrt.
500 Internal Server Error	Nicht-HTTP-bezogener Fehler. Ein Request konnte vom Server aufgrund eines internen Fehlers nicht bearbeitet werden.

Tabelle 7: HTTP-Statuscodes

Die Kundendaten stehen zusätzlich im JSON-Format an der HAN-Schnittstelle zur Verfügung.
Diese Daten können (z. B. mittels eines Energiemanagementsystems) nur mit den Zugangsdaten des Letztverbrauchers abgerufen werden.

5.1 Kommunikationsverbindung mit CASA Benutzerportal einrichten

In diesem Abschnitt wird beschrieben, wie Sie über Ihr Auslesegerät (Laptop oder PC) eine Verbindung mit dem CASA herstellen. Dazu wird ein abgeschirmtes Netzwerkkabel benötigt.

Auf dem Auslesegerät muss ein Internet Browser installiert sein, welcher verschlüsselte Verbindungen gemäß dem TLS-Protokoll Version 1.2 unterstützt.

Die Benutzung des Chrome-Browsers wird empfohlen.

Der CASA überwacht und beschränkt die Anzahl erfolgloser Anmeldeversuche. Wird die maximal zulässige Anzahl der fehlerhaften Anmeldeversuche überschritten, ist ein neuer Anmeldeversuch erst nach 5 Minuten möglich.

Die Anzahl der fehlerhaften Anmeldeversuche für den Letztverbraucher bezieht sich auf den gesamten Letztverbraucherzugang.

Bei Fragen hierzu wenden Sie sich bitte an Ihren Messstellenbetreiber.

Hinsichtlich der Schnittstelle des CASA nutzen Sie eine der folgenden Möglichkeiten:

- HAN (siehe Kapitel 2.3 / Seite 13)
- [HAN] CLS (siehe Kapitel 2.3 / Seite 13)
- eine anderweitig von Ihrem Messstellenbetreiber bereitgestellte HAN-Schnittstelle

Um eine Verbindung mit dem CASA einzurichten, verfahren Sie wie folgt:

1. Stecken Sie ein abgeschirmtes Netzwerkkabel an die Ethernet-Buchse der gewählten HAN-Schnittstelle, bis der Stecker einrastet.
2. Das andere Ende des Netzwerkkabels stecken Sie an die Netzwerkbuchse Ihres Laptops oder PCs.

Ihr Computer und der CASA müssen sich im selben IP-Netzbereich befinden. Sofern die IP-Adresse der benutzten HAN-Schnittstelle nicht vom Messstellenbetreiber vorgegeben wurde, ist die IP-Adresse vom Hersteller wie folgt voreingestellt:

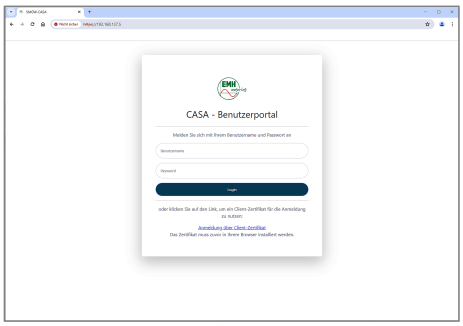
IPv4: `192.168.137.2`

Subnetz: `255.255.255.0`

Falls die IP-Adresse des CASA auf Wunsch des Messstellenbetreibers anders konfiguriert wurde, wenden Sie sich bitte an den Messstellenbetreiber.

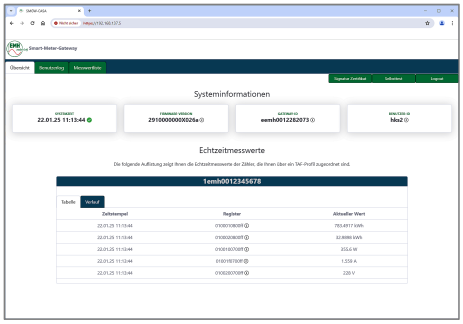
3. Öffnen Sie den Internet Browser auf Ihrem Gerät und geben Sie in die Adressleiste des Browsers die IP-Adresse der gewählten HAN-Schnittstelle des CASA im Format ***https://ip-Adresse*** ein.
   Alternativ können die Hostnamen ***smgw.local*** und ***<HUID>.local*** verwendet werden, wobei ***<HUID>*** der herstellerübergreifenden ID des CASA entspricht. Beispiel: ***https://eemh0009264154.local***

▶ Der Anmeldebildschirm des CASA-Benutzerportals wird angezeigt.
(Eine eventuell erscheinende Sicherheits- bzw. Warnmeldung Ihres Browsers können Sie ignorieren. Ursache hierfür ist ein selbstsigniertes TLS-Zertifikat, welches der CASA an der HAN-Schnittstelle verwendet.)

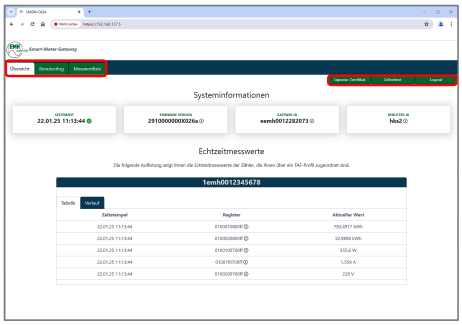


4. Wählen Sie die gewünschte Authentifizierungsmethode, z. B. die [Benutzername / Passwort] -Kombination, die Sie von Ihrem Messstellenbetreiber erhalten haben. Nachfolgend wird der Zugang über Benutzername / Passwort beschrieben.
   (Alternativ erfolgt der Zugang per Client-Zertifikat, welches Sie von Ihrem Messstellenbetreiber erhalten haben.)
5. Geben Sie Benutzername und Passwort ein.
6. Klicken Sie auf die Schaltfläche [Login].

▶ Die Startseite des CASA-Benutzerportals wird angezeigt (Beispiel).



In und unter der Titelleiste befinden sich drei Registerkarten (links) und drei Schaltflächen (rechts). Die damit korrespondierenden Funktionen und Ansichten werden in den nächsten Kapiteln beschrieben.



Zum Vor- oder Zurücknavigieren im CASA-Benutzerportal können Sie die Funktionen Ihres Browsers nutzen.

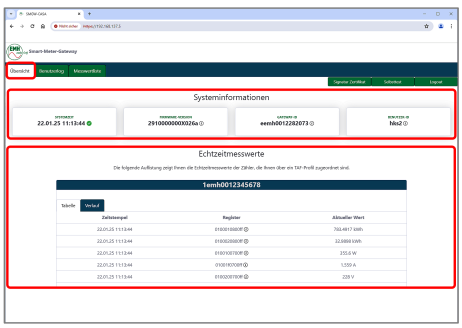
Bitte beachten Sie, dass die Verwendung der Browser-Funktionen „Seite neu laden“ bzw. „Refresh“ (Taste F5) eine erneute Anmeldung notwendig macht.

Nach 10-minütiger Inaktivität werden Sie automatisch vom CASA-Benutzerportal abgemeldet.

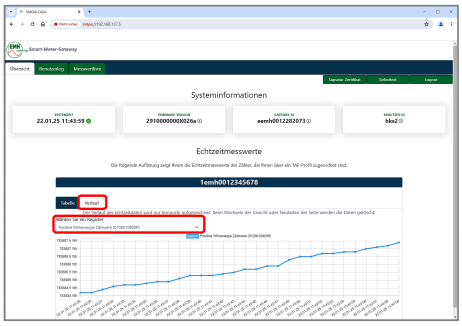
5.2 CASA-Benutzerportal – Übersicht

Auf dem Bildschirm [Übersicht] werden Ihnen im oberen Bereich aktuelle Systeminformationen (Systemzeit, Firmwareversion, HüID sowie Ihre Benutzer-ID) angezeigt.

Im unteren Bereich des Bildschirms [Übersicht] werden die Echtzeitmesswerte der Zählerregister angezeigt, welche Ihnen als Letztverbraucher über ein TAF-Profil zugeordnet sind.



Die Darstellung der Echtzeitmesswerte erfolgt wahlweise als [Tabelle] oder als grafischer [Verlauf]. Die Umschaltung erfolgt per Mausklick.



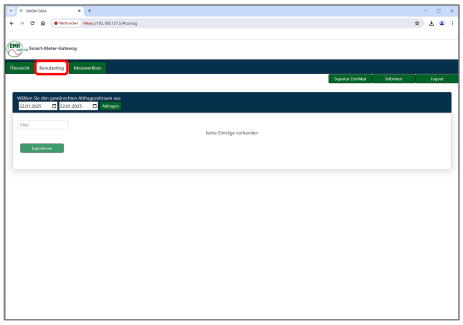
In der Ansicht [Verlauf] erfolgt sekündlich eine Aktualisierung der grafischen Anzeige.
Über die Dropdown-Liste wählen Sie das gewünschte Register, welches angezeigt wird.

5.3 CASA-Benutzerportal – Benutzerlog

Das Letztverbraucher-Log (auf dem Benutzerportal als „Benutzerlog“ bezeichnet) zeigt alle Ereignisse an, die rechtlich relevant sind (z. B. Neustarts des CASA, Uhrsynchronisation, veränderte Tarifprofile). Zudem werden alle Ereignisse angezeigt, die den Datenfluss der Ihnen als Letztverbraucher zugeordneten Daten beschreiben, wie z. B. der Versand von Messdaten an externe Marktteilnehmer.

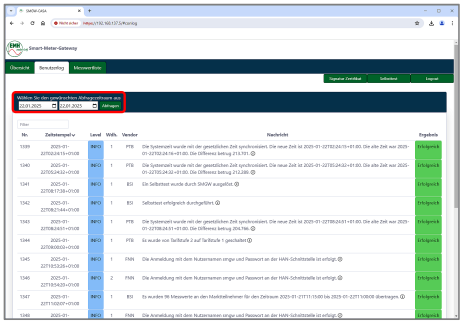
☞ Um das Letztverbraucher-Log auszulesen:

1. Wechseln Sie zur Funktion [Benutzerlog] in der Titelleiste des CASA-Benutzerportals.

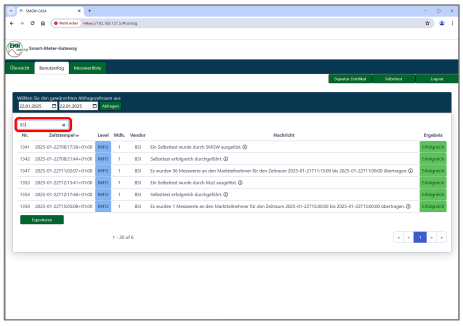


2. Wählen Sie den Auslesezeitraum und klicken Sie auf [Abfragen].

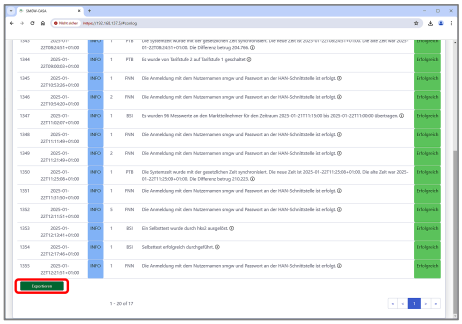
▶ Das Letztverbraucher-Log wird in tabellarischer Form dargestellt.



3. Optional können Sie die angezeigten Einträge über die Filterfunktion auf beliebige Schlüsselwörter filtern (im abgebildeten Beispiel: BSI).



4. Falls gewünscht, können Sie die für den Auslesezeitraum angezeigten Daten in eine CSV-Datei herunterladen. Hierzu navigieren Sie an das Ende der Seite und klicken Sie auf die Schaltfläche [Exportieren].



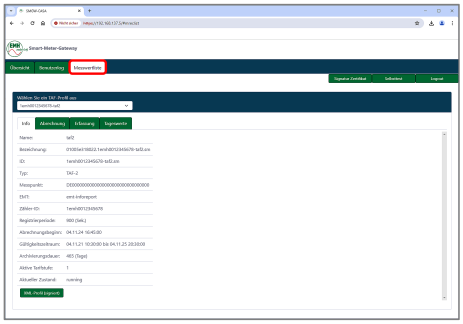
▶ Die CSV-Datei wird im Download-Verzeichnis Ihres Browsers gespeichert.

5.4 CASA-Benutzerportal – Messwertliste

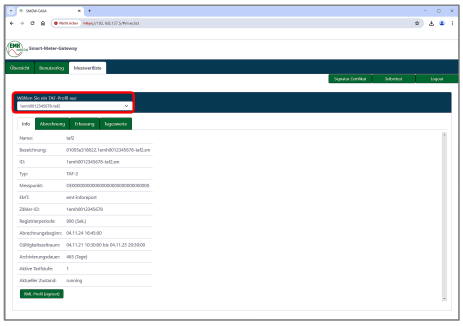
Über die Funktion [Messwertliste] können die für die Tarifierung relevanten Informationen und Messwerte abgerufen werden.

☞ Um die Messwertliste zu einem gewünschten Tarifanwendungsfall (TAF) auszulesen, gehen Sie wie folgt vor:

1. Wechseln Sie zur Funktion [Messwertliste] in der Titelleiste des CASA-Benutzerportals.

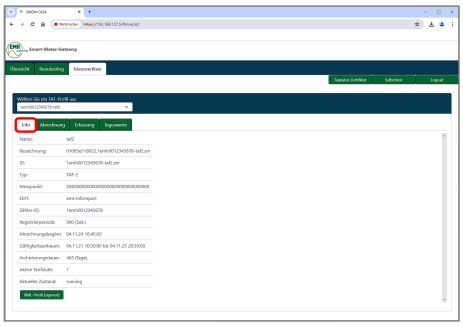


2. Wählen Sie das gewünschte TAF-Profil aus der Dropdown-Liste.

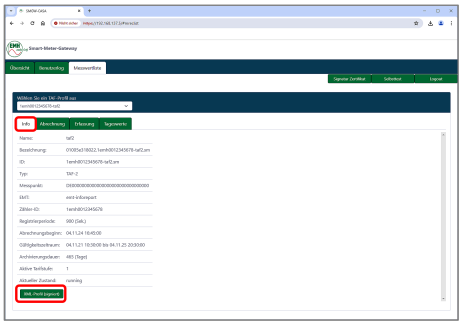


5.4.1 Info

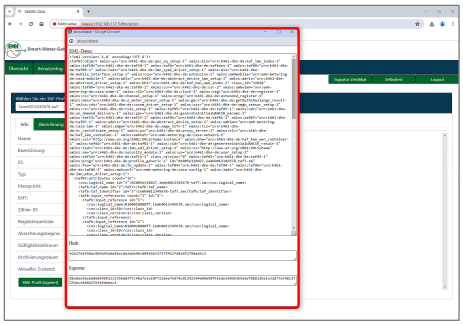
In der Ansicht [Info] werden alle relevanten Parameter des gewählten TAF-Profils angezeigt.



Über die Schaltfläche [XML-Profil (signiert)] kann das vom Gateway-Administrator eingespielte und vom CASA signierte Profil im originalen XML-Format angezeigt werden.



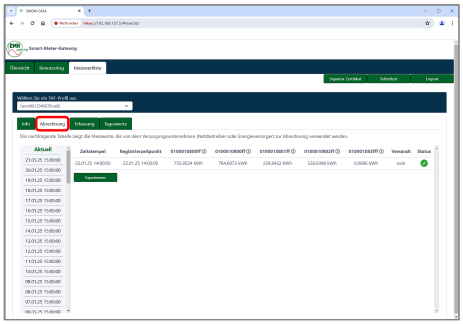
Beispiel für die Anzeige des XML-Profils (Popup-Fenster):



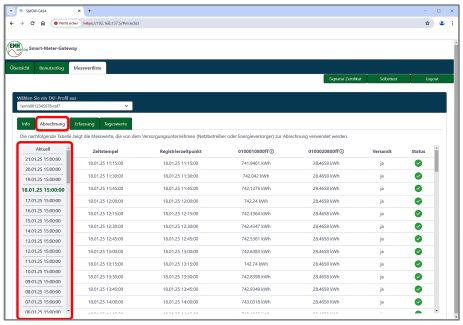
5.4.2 Abrechnung

Die Ansicht [Abrechnung] ist nur für abrechnungsrelevante TAF-Profile verfügbar.

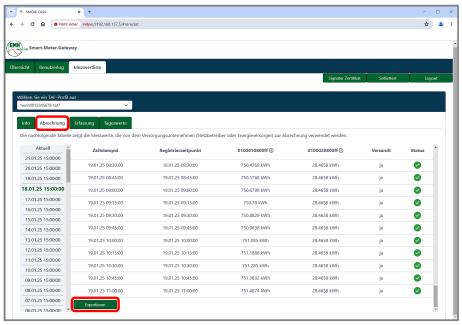
In der Ansicht [Abrechnung] werden alle für die Abrechnung relevanten Messwerte inklusive der Messwertstatus in tabellarischer Form dargestellt (abgeleitete Messwertliste).



In der linken Spalte des Anzeigebereichs kann der gewünschte Abrechnungszeitraum per Mausklick gewählt werden.



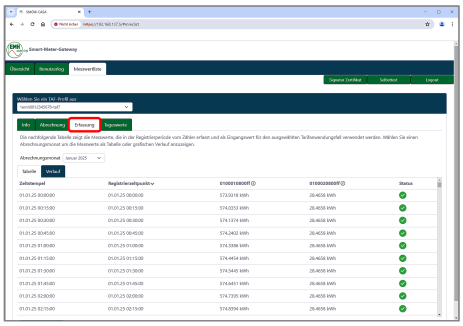
Über die Schaltfläche [Exportieren] am Ende der Seite können die Daten des gewählten Abrechnungszeitraums in eine CSV-Datei heruntergeladen werden.



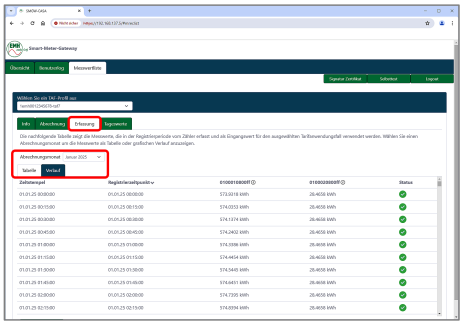
5.4.3 Erfassung

Die Ansicht [Erfassung] ist nur für abrechnungsrelevante TAF-Profile verfügbar.

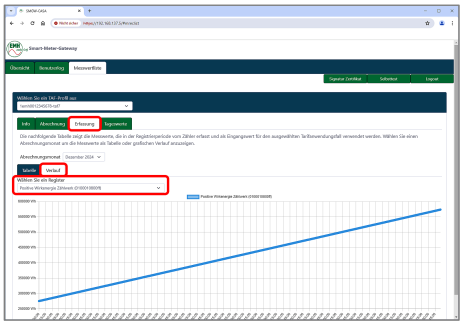
In der Ansicht [Erfassung] werden alle für die Abrechnung relevanten Messwerte, die im Raster der Registrierperiode für den Zähler erfasst wurden, dargestellt (originäre Messwertliste).



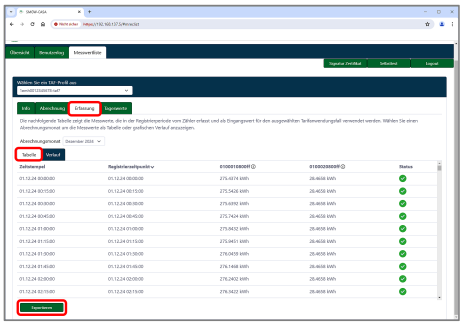
Der Abrechnungsmonat kann gewählt, zwischen tabellarischer und grafischer Darstellung kann gewechselt werden.



Bei grafischer Darstellung kann ein gewünschtes Register aus der Dropdown-Liste ausgewählt werden.



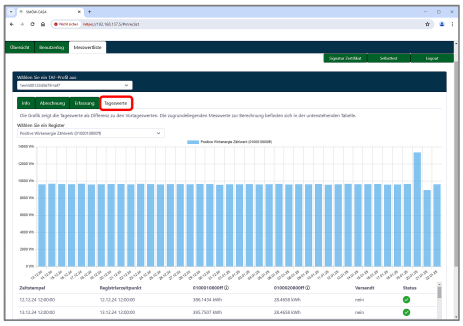
Bei tabellarischer Darstellung können die Daten des gewählten Abrechnungszeitraums in eine CSV-Datei heruntergeladen werden. Die Schaltfläche [Exportieren] befindet sich am Ende der Seite.



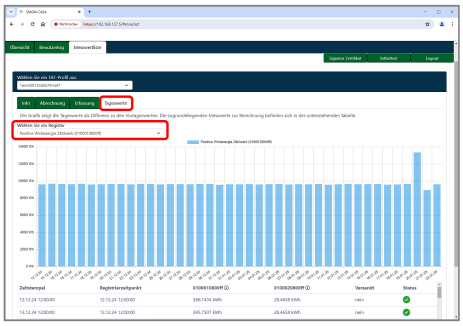
5.4.4 Tageswerte

Die Ansicht [Tageswerte] ist nur für abrechnungsrelevante TAF-Profile verfügbar.

In der Ansicht [Tageswerte] werden die Messwerte, die zu Beginn jedes Abrechnungstages erfasst werden, im unteren Bereich des Fensters tabellarisch dargestellt.
Im oberen Bereich erfolgt die grafische Ansicht der Differenz von aufeinanderfolgenden Messwerten. Somit kann der Tagesverbrauch für den jeweiligen Messwert ermittelt werden. Die auf diese Weise ermittelten Werte dienen nur der Übersicht, sie sind selbst nicht abrechnungsrelevant.



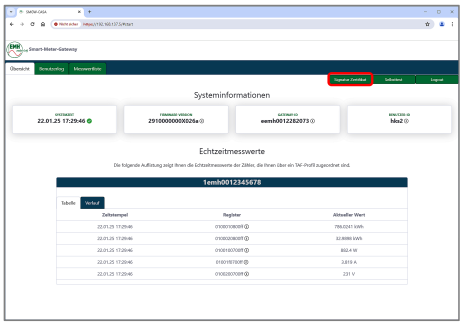
Das gewünschtes Register kann aus der Dropdown-Liste ausgewählt werden.



5.5 CASA-Benutzerportal – Signatur-Zertifikat

Das Signatur-Zertifikat dient zur Überprüfung der Authentizität von Zählerwerten aus der Messwertliste.

Um das aktuelle Signatur-Zertifikat des CASA herunterzuladen:
Wechseln Sie zur Funktion [Signatur-Zertifikat].



▶ Das Signatur-Zertifikat wird im Download-Verzeichnis Ihres Browsers gespeichert.

5.6 CASA-Benutzerportal – Selbsttest

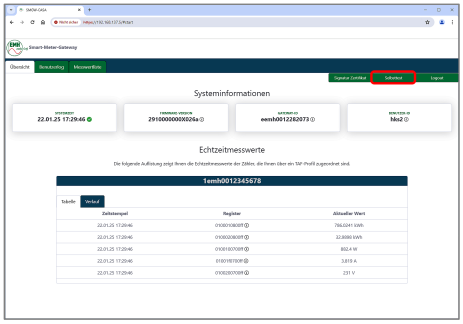
Der Selbsttest des CASA dient dazu, die korrekte Funktion des Gerätes zu überprüfen.

Der Selbsttest kann innerhalb von 24 Stunden einmalig ausgeführt werden. Beim Versuch, innerhalb von 24 Stunden einen weiteren Selbsttest auszulösen, erscheint eine Meldung mit dem Datum und der Uhrzeit, zu welcher der weitere Selbsttest frühestens ausgeführt werden kann.
Die Begrenzung dient dazu, eine übermäßige Belastung des CASA zu vermeiden.

Je nach Auslastung des CASA kann der Selbsttest einige Zeit in Anspruch nehmen.

☞ Um bei Bedarf einen Selbsttest auszulösen:

Wechseln Sie zur Funktion [Selbsttest].



▶ Das Ergebnis des Selbsttests finden Sie anschließend im Letztverbraucher-Log, siehe Kapitel 5.3 / Seite 35.

Während des Selbsttests können einige Fehler auftreten, die den CASA in den Soft Lock-Down Modus versetzen (siehe Kapitel 5.8 / Seite 41).

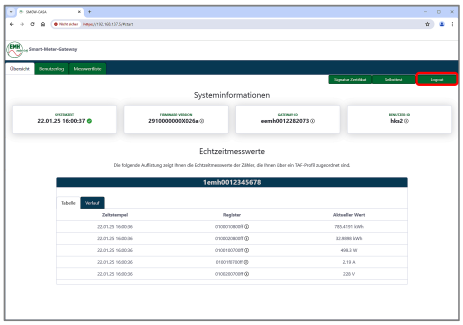
In diesem Fall kann das Ergebnis des Selbsttests über das CASA-Benutzerportal erst aufgerufen werden, nachdem der bzw. die Fehler vom Gateway-Administrator behoben wurde(n).

5.7 CASA-Benutzerportal – Logout

Nach 10-minütiger Inaktivität werden Sie automatisch vom CASA-Benutzerportal abgemeldet.

Mit der Abmeldung vom CASA-Benutzerportal ist die Löschung sämtlicher im Browser gespeicherten Session-Daten verbunden.

☞ Um sich vom CASA-Benutzerportal abzumelden, klicken Sie auf die Funktion [Logout].



▶ Sie werden abgemeldet und der Anmeldebildschirm des CASA-Benutzerportals wird angezeigt.

5.8 Fehlerzustand

Die Behebung von Fehlern erfolgt ausschließlich durch den Gateway-Administrator oder auf dessen Anweisung.

Im CASA aufgetretene Fehler werden an den LEDs signalisiert (siehe Kapitel 2.3.1 / Seite 13) und im Letztverbraucher-Log vermerkt (siehe Kapitel 2.9.2.1 / Seite 23).

Beim Auftreten von Fehlermeldungen im Letztverbraucher-Log informieren Sie als Letztverbraucher bitte den Messstellenbetreiber (siehe Kapitel 6.3 / Seite 46). Der Messstellenbetreiber beauftragt den Gateway-Administrator mit Maßnahmen zur Fehleranalyse und Fehlerbehebung.

Stellt der CASA im Rahmen des Selbsttests einen Fehler fest, durch den er seinen normalen Betriebsmodus nicht mehr ausführen kann, geht er in den Soft Lock-Down Modus bzw. in den Hard Lock-Down Modus (siehe Kapitel 2.8 / Seite 19). Die betreffenden Fehler lassen sich der Tabelle in Kapitel 6.3 / Seite 46 entnehmen. Der Gateway-Administrator wird automatisch informiert.

In diesen Fällen ist eine Anmeldung an einer der HAN-Schnittstellen nicht möglich. Somit können keine personenbezogene Daten (Messwerte, Log-Einträge) abgerufen werden.

Dieser Zustand wird im CASA-Benutzerportal durch folgenden Hinweistext dargestellt:

6 Anhang

6.1 CASA-Software

Der CASA enthält Software, die unter der General Public Licence (GPL) steht.

Weitere Informationen hierzu können unter folgender Adresse abgerufen werden:
http://www.gnu.org/copyleft/gpl.html
Der CASA enthält Open Source Komponenten. Nähere Informationen erhalten Sie auf Anfrage.

6.2 Protokollierte Ereignisse

Die folgenden Unterkapitel enthalten alle Ereignisse, die in das Letztverbraucher-Log geschrieben werden.

Die im Text enthaltenen Zahlen in eckigen Klammern (z. B. [1] oder [2]) sind Platzhalter für Inhalte, die je nach Ereignis vom CASA eingefügt werden.

Beim Auftreten von Fehlermeldungen unternimmt der Gateway-Administrator geeignete Schritte zur Behebung des Fehlers.

6.2.1 LMN

event_id	event_sub_id	Log Level	Text der Meldung
1011	1	error	Der Zähler [1] hat einen temporären Messwert-Fehlerstatus ([2]) gemeldet.
1011	2	error	Der Zähler [1] hat einen fatalen Messwert-Fehlerstatus ([2]) gemeldet.

6.2.2 HAN-Schnittstelle + CLS-Gerät

event_id	event_sub_id	Log Level	Text der Meldung
5001	0	info	Die Anmeldung mit dem Nutzernamen [1] und Passwort an der HAN-Schnittstelle ist erfolgt.
5001	1	warning	Die Anmeldung mit dem Nutzernamen [1] und Passwort an der HAN-Schnittstelle ist fehlgeschlagen. Die Anmeldeinformationen sind ungültig.
5001	2	error	Die Anmeldung mit dem Nutzernamen [1] und Passwort an der HAN-Schnittstelle ist fehlgeschlagen. Es ist folgender Fehler aufgetreten: [2]
5002	0	info	Die Anmeldung mit einem Benutzerzertifikat mit der Subject-ID [1] (Aussteller [2]) an der HAN-Schnittstelle ist erfolgt.
5002	1	warning	Die Anmeldung mit einem Benutzerzertifikat mit der Subject-ID [1] (Aussteller [2]) an der HAN-Schnittstelle ist fehlgeschlagen. Das Zertifikat ist ungültig oder nicht vertrauenswürdig.
5002	2	error	Die Anmeldung mit einem Benutzerzertifikat mit der Subject-ID [1] (Aussteller [2]) an der HAN-Schnittstelle ist fehlgeschlagen. Es ist folgender Fehler aufgetreten: [3]

6.2.3 Operative Betriebsbereitschaft

Die Log-Meldungen mit der Event-ID 6001 tritt nur beim CASA 1.1 auf, nicht beim CASA 1.0.

event_id	event_sub_id	Log Level	Text der Meldung
6001	0	info	Die Wiederkehr der Betriebsspannung wurde erkannt.

6.2.4 Zeitsynchronisation

event_id	event_sub_id	Log Level	Text der Meldung
13001	1	error	Die Systemzeit des SMGW wird als ungültig angenommen.
13002	0	info	Die Systemzeit des SMGW wurde gestellt. Die neue Zeit ist [1]. Die alte Zeit war [2]. Die Differenz betrug [3] Millisekunden.
13003	0	info	Die Systemzeit wurde mit der gesetzlichen Zeit synchronisiert. Die neue Zeit ist [1]. Die alte Zeit war [2]. Die Differenz betrug [3].
13005	1	error	Die Synchronisation der Systemzeit mit der gesetzlichen Zeit hat eine Differenz von [1] Sekunden ergeben. Die zulässige Fehlertoleranz von 3% der kleinsten Registrierperiode wurde damit überschritten.
4294954294	0	info	Die Systemzeit des SMGW wurde unter Verwendung der RTC gestellt. Die neue Zeit ist [1].

6.2.5 Selbsttest

event_id	event_sub_id	Log Level	Text der Meldung
15001	0	info	Selbsttest erfolgreich durchgeführt.
15001	1	fatal	Selbsttest fehlgeschlagen. Es wurden [1] Fehler erkannt. Es sind folgende Fehler aufgetreten: [2]
15002	0	info	Ein Selbsttest wurde durch [1] ausgelöst.
15002	1	info	Ein Selbsttest konnte durch [1] nicht ausgelöst werden. Es ist folgender Fehler aufgetreten: [2]

6.2.6 Messwertübertragung

event_id	event_sub_id	Log Level	Text der Meldung
16001	0	info	Es wurden [1] Messwerte an den Marktteilnehmer für den Zeitraum [2] bis [3] übertragen.
16002	0	info	Die Messwerte für die Erstauslesung zum Zeitpunkt [1] wurden an den Marktteilnehmer übertragen.
16003	0	info	Die Messwerte für die Endablesung zum Zeitpunkt [1] wurden an den Marktteilnehmer übertragen.
16004	0	info	Es wurde eine Bedarfsauslesung an Tag [1] für das Auswerteprofil für den Marktteilnehmer [2] ausgelöst.
16004	4	warning	Es wurde eine Bedarfsauslesung an Tag [1] für das Auswerteprofil ausgelöst. Der empfangene Marktteilnehmer ([2]) ist nicht in dem Auswerteprofil referenziert!
16005	0	info	Es wurden [1] Messwerte an den Marktteilnehmer für eine Bedarfsauslesung am [2] übertragen.

6.2.7 Funktionsüberprüfung

event_id	event_sub_id	Log Level	Text der Meldung
19001	1	fatal	Die Integrität des SMGW wurde verletzt oder kann nicht mehr sichergestellt werden. Es ist folgender Fehler aufgetreten: [1]
19004	0	info	Der Startvorgang der SMGW-Firmware wurde abgeschlossen.
19005	1	error	Der Messbetrieb wurde eingestellt.
19006	0	info	Der Messbetrieb wurde aufgenommen.
19006	1	warning	Bei der Erfassung oder Verarbeitung von Messwerten ist folgende Warnung aufgetreten: [1]
19006	2	error	Bei der Erfassung oder Verarbeitung von Messwerten ist der Fehler [1] aufgetreten.
19007	2	error	Die Speicherkapazität ist erschöpft. Das Gerät muss ausgewechselt werden.
19008	2	fatal	Die Kapazität des Eich-Logs ist erschöpft. Das Gerät muss ausgetauscht werden.
4294948294	1	warning	Letztverbraucher-Log für [1] ist voll. Einträge älter als 15 Monate wurden gelöscht.
4294948293	1	warning	Es wurden [1] oder mehr ungültige Authentifizierungsversuche registriert ([2]).
4294948286	1	fatal	Es ist der fatale Fehler [1] im System aufgetreten. Der Hash der Fehlermeldung lautet [2]. Das Gerät wechselt in den Soft Lock-Down Modus.
4294948285	0	Info	Das Gerät wird heruntergefahren und neu gestartet.
4294948284	1	warning	Es wurde in der Log-Datei [1] ein unvollständiger Eintrag gefunden.

event_id	event_sub_id	Log Level	Text der Meldung
4294948266	2	warning	Das System ist zum ersten Mal oder nach einem unerwarteten Reboot gestartet (Fehlercode: [1]).

6.2.8 Profilkonfiguration

event_id	event_sub_id	Log Level	Text der Meldung
20003	0	info	Das Kommunikationsprofil [1] wurde aktualisiert. Die Zieladressen sind [2].
20010	0	info	Das Auswerteprofil [1] wurde angelegt.
20011	0	info	Das Auswerteprofil [1] wurde aktualisiert.
20012	0	info	Das Auswerteprofil [1] wurde beendet.
20013	0	info	Das Auswerteprofil [1] wurde gelöscht.
20018	0	info	Die CLS-EMT Verbindung durch das Proxyprofil [1] wurde erfolgreich aufgebaut.
20020	0	info	Die CLS-EMT Verbindung durch das Proxyprofil [1] wurde erfolgreich abgebaut.
20029	0	info	Das Auswerteprofil [1] wurde von dem Gatewayadministrator ausgelesen.
20030	0	info	Das Sensorprofil [1] wurde von dem Gatewayadministrator ausgelesen.
20032	0	info	Das Endedatum wurde auf [1] korrigiert.
20033	0	info	Die Zugangsdaten im Kommunikationsprofil [1] wurden aktualisiert.

6.2.9 Messwertverarbeitung

event_id	event_sub_id	Log Level	Text der Meldung
21002	0	info	Es wurde von Tarifstufe [1] auf Tarifstufe [2] geschaltet.
4294946295	0	info	Der TAF [1] mit den/dem Zähler(n) [2] wurde gestartet.

6.3 Herstellerspezifische Fehlercodes

In der nachfolgenden Tabelle sind alle Fehlercodes aufgelistet, die innerhalb einer Logmeldung oder als Ergebnis eines Selbsttests auftreten können.

Alle Fehler, die in der Spalte „Soft Lock-Down Modus“ mit einem **x** markiert sind, versetzen den CASA beim Auftreten in den Soft Lock-Down Modus.

☞ Tritt ein Fehler innerhalb einer Logmeldung oder als Ergebnis eines Selbsttests auf, informieren Sie als Letztverbraucher bitte den Messstellenbetreiber. Dieser beauftragt den Gateway-Administrator mit Maßnahmen zur Fehleranalyse und Fehlerbehebung.

Fehlercode	Beschreibung	Soft Lock-Down Modus
103165	TLS Verbindungsfehler, Rückfall auf SYM Pairing	
103190	HDLC Lese-Timeout abgelaufen, Zähler nicht empfangsbereit	
103191	HDLC Lese-Timeout abgelaufen	
103106	Empfangenes HDLC Frame kann nicht dekodiert werden	
103117	Nicht erwartetes HDLC Frame empfangen	
103118	Keine HDLC Antwort erhalten	
100701	Interne Prozesskommunikation gestört	
100702	RS485 Aktivierungszustand nicht wie erwartet	
100703	RS485 Aktivierungszustand nicht wie erwartet	
100704	SMGW LMN TLS Zertifikat läuft innerhalb von 6 Monaten ab	
100705	LMN TLS Zertifikat(e) läuft / laufen innerhalb von 6 Monaten ab	
100706	Keine Kommunikation mit Zähler, Verbindung wird neu aufgebaut	
200704	Interne Prozesskommunikation gestört	
200701	Der Kommunikationsport zum wM-Bus Modul ist nicht geöffnet	
200702	Der Kommunikationsport zum wM-Bus Modul ist falsch konfiguriert	
200507	Fehler bei Kommunikation mit wM-Bus Modul	
200509	Falsche Firmwareversion auf wM-Bus Modul erkannt	
200504	Fehler bei Kommunikation mit wM-Bus Modul	
200505	Falsche wM-Bus Modulbezeichnung erkannt	
200506	Falsche Firmwareversion auf wM-Bus Modul erkannt	
200710	Neustart des wM-Bus Moduls nicht erfolgreich	
1800200	CLS-Socks-Server nicht gestartet	
1800201	Interne Prozesskommunikation gestört	
1800202	Kein gültiges SMGW HAN-Zertifikat (BP)	
1800122	Verbindung konnte nicht aufgebaut werden	
1800123	Verbindung konnte nicht aufgebaut werden: Timeout	
800802	CON-Server kann keine Anfragen entgegennehmen	
800803	CON-Server kann keine Anfragen entgegennehmen	
800805	Interne Prozesskommunikation gestört	
400001	Zugehöriges TAF-Profil nicht gefunden	
400033	Logical_name des OnDemandDelivery-Profils ungültig	
400034	Referenziertes TAF-Profil nicht gefunden	
400035	Referenziertes TAF-Profil nicht gefunden	
400036	Fehler beim Übertragen der Daten	
400105	Interne Prozesskommunikation gestört	
400107	Interne Prozesskommunikation gestört	

Fehlercode	Beschreibung	Soft Lock-Down Modus
400109	Verbindungsfehler beim Versenden von Messwerten	
400110	Gegenstelle meldet Fehler beim Versenden von Messwerten	
400101	Keine Messwerte zum Übertragen vorhanden	
400111	Fehler bei der Bearbeitung der Messwertversandvorgänge	
700034	Ein am GWA-Wechsel beteiligter Dienst hat den GWA-Wechsel abgebrochen	
700501	Prozess nicht korrekt initialisiert	
700502	Interne Prozesskommunikation gestört	
700503	MGMT-Verbindungsstatus inkonsistent	x
500007	Prozess nicht korrekt initialisiert	
500008	Interne Prozesskommunikation gestört	
900133	Interne Prozesskommunikation gestört	
900135	WAN und HAN vertauscht	x
900137	WAN und HAN verbunden	x
900138	Firewall-Regeln inkonsistent	x
900139	Firewall-Regeln inkonsistent	x
900140	HAN-Schnittstelle hat ein Standard Gateway konfiguriert	x
900141	Firewall-Regeln inkonsistent	x
900072	Initialisierung (Loop-Test) der HAN-Schnittstelle fehgeschlagen	x
901000	Unbekannter Fehler	
901001	Netzwerkfehler: No Carrier	
901002	Netzwerkfehler: DeRegistration	
901003	Netzwerkfehler: Detach	
901004	Netzwerkfehler: Only emergency	
901005	Nicht im Netz registriert	
901006	Schlechte Signalstärke	
901007	Schlechte Signalqualität	
901008	Schlechte IP-Qualität	
901009	Fehlende IP-Adresse	
901010	TX/RX -Fehler	
901011	SIM-Fehler	
901012	Modem-Fehler	
901013	PPP idle time	
901014	Modem-Konfiguration wurde geändert	
901015	Keine IP-Verbindung	
901016	APN-Wechsel wurde angestoßen	
901017	Reset durch LWM2M	
901018	FOTA durch LWM2M	
901019	Fehler in der LWM2M-Applikation	
901200	Nicht registriert	
901201	Registriert im Heimatnetz	
901202	nicht registriert, Netz wird gesucht	
901203	Registrierung abgewiesen	
901205	Registriert imRegistriert im Roamingnetz Roamingnetz	
901206	Nur für SMS registriert	
901211	Nur für Notrufe registriert	

Fehlercode	Beschreibung	Soft Lock-Down Modus
901301	unbekannter Fehler beim APN-Wechsel	
901302	pppd Fehler	
901303	PDP-Kontext konnte nicht aufgebaut werden	
901311	Schnittstellenfehler bei LwM2M-App	
901312	Protokollfehler bei LwM2M-App	
901313	Timeoutfehler bei Nachricht zu LwM2M-App	
901314	Timeoutfehler bei LwM2M-App	
901315	Ablauffehler bei LwM2M-App	
901316	APN durch LwM2M-App nicht gesetzt	
901317	Fehlercode von LwM2M-App	
900151	Initialisierung der WAN-Schnittstelle fehlerhaft	
900152	Konfiguration der WAN-Schnittstelle fehlerhaft	
901400	Modem-Fehler im unbekannten Zustand	
901401	Modem-Fehler im Zustand 'Fehler'	
901402	Modem-Fehler im Zustand 'Modem-Reset'	
901403	Modem-Fehler im Zustand 'Verzögerung Modem-Initialiserung'	
901404	Modem-Fehler im Zustand 'Modem-Initialiserung'	
901405	Modem-Fehler im Zustand 'SIM-PIN Prüfung'	
901406	Modem-Fehler imZustand 'SIM-Initialisierung'	
901407	Modem-Fehler im Zustand 'Providerauswahl'	
901408	Modem-Fehler im Zustand 'MUXER'	
901409	Modem-Fehler im Zustand 'PPPD-Konfiguration'	
901410	Modem-Fehler im Zustand 'PPPD'	
901411	Modem-Fehler im Zustand 'Running'	
901412	Modem-Fehler im Zustand 'Modem-Deaktivierung'	
2200041	Das Zertifikat ist abgelaufen	
2200042	Das Zertifikat hat seinen Gültigkeits-Startzeitpunkt noch nicht erreicht	
2200044	Ein Benutzer mit dem angegebenen Zertifikat existiert nicht	
2300033	Entschlüsselung der CMS-Daten fehgeschlagen	
2300035	Signieren der CMS-Daten fehlgeschlagen	
2300026	Komprimierung der CMS-Daten fehlgeschlagen	
2300097	Nicht ausreichend Speicher verfügbar	
2300098	Interner TLS-Fehler	
2300151	Entpacken der CMS-Daten fehlgeschlagen	
2300171	Fehlerhafte CMS-Signatur	
2300160	Verschlüsselung der CMS-Daten fehgeschlagen	
2300300	Auslesen des GWA Common Name für neue OU fehlgeschlagen	
2300301	Erstellen einer einzelnen CertReqMsg fehlgeschlagen	
2300302	Erstellen der CertReqMessages Sequenz fehlgeschlagen	
2300303	Erstellen des vollständigen CSR Containers fehlgeschlagen	
2300304	Laden der Schlüssel-Objekte aus dem Sicherheitsmodul fehlgeschlagen	
2300305	Ungültiges Issuer-Zertifikat	
2300306	Austellerzertifikat nicht vertrauenswürdig	
1400001	Es wurden doppelte Logfiles gefunden, der Fehler wurde behoben	
1400002	Logdatei-Nummerierung inkonsistent	x

Fehlercode	Beschreibung	Soft Lock-Down Modus
1400003	Logdatei-Nummerierung inkonsistent	x
1400005	Integritätscheck der Logbücher fehlgeschlagen	x
1400008	Interne Prozesskommunikation gestört	
1400009	Eine Hash-Datei konnte nicht geöffnet werden	x
1400010	Eine Hash-Datei konnte nicht gefunden werden	x
1400011	Bei der Überprüfung der Logdatei-Anzahl wurde ein Fehler festgestellt	x
1400012	Integritätscheck der Logbücher fehlgeschlagen	x
1400013	Eine Logdatei konnte nicht geöffnet werden	x
1400560	Fehlerhafte Dateiattribute gefunden	x
1400509	Interner Fehler im Logsystem	x
1400513	Fehler beim Schreiben eines Logeintrages	x
1400514	Fehler beim Erzeugen einer neuen Logdatei	x
1400515	Interner Fehler im Logsystem	x
1400516	Interner Fehler im Logsystem	x
1400517	Fehler beim Schreiben eines Logeintrages	x
1400518	Fehler beim Schreiben eines Logeintrages	x
1400523	Löschen von Logdaten nicht möglich, da nicht älter als 15 Monate	x
1400550	Integritätsfehler bei Systemstart festgestellt	x
1400551	Fehler bei der Überprüfung der Anzahl der Logdateien	x
1400552	Integritätsfehler beim Erstellen einer neuen Logdatei festgestellt	x
1400014	Der Login-Prozess ist gestoppt	
1700018	Interner Prozessfehler	
1700019	Interne Prozesskommunikation gestört	
1700020	eMMC Wartung gestört	
1700105	eMMC Wartung gestört	
1700107	eMMC Wartung nicht aktiv	
1100025	Interne Prozesskommunikation gestört	
1100026	Interne Prozesskommunikation gestört	
1100027	Interne Prozesskommunikation gestört	
1100028	Interne Prozesskommunikation gestört	
600026	Originalprofil konnte nicht ausgelesen werden	
600028	Fehler beim Erkennen des Profiltyps	
600029	Fehler beim XML-Codieren des Profils	
600032	Interner Konfigurationsfehler	
600033	Konfigurationssynchronisation gestört	x
600034	Konfiguration setzen gestört	
600035	Konfiguration lesen gestört	
600036	Konfiguration löschen gestört	
600037	Kein Konfigurationsobjekt	
600038	Konfigurationssynchronisation gestört	
600039	Konfigurationssynchronisation gestört	x
600040	Konfigurationssynchronisation gestört	
600041	Konfiguration setzen gestört	
600042	Konfiguration lesen gestört	
600043	Konfiguration löschen gestört	

Fehlercode	Beschreibung	Soft Lock-Down Modus
600044	Konfigurationssynchronisation gestört	
600045	Konfigurationssynchronisation gestört	
600104	Profilvalidierung fehlgeschlagen	
600214	Integritätsprüfung fehlgeschlagen	x
600215	Integritätsprüfung fehlgeschlagen	x
1900001	Es sind nicht alle benötigten SMGW-Dienste gestartet	
1900004	Eine Smack-Regel wurde verletzt	x
1900008	Der Selbsttest eines SMGW-Dienstes konnte nicht gestartet werden	x
1900010	Kritischer Fehler während eines Selbstest gefunden	x
1900082	Nur noch wenig Speicherplatz vorhanden	x
1900109	Integritätscheck des Dateisystems fehlgeschlagen	x
1900110	Integritätscheck des Dateisystems fehlgeschlagen	x
1900112	Integritätscheck des Dateisystems fehlgeschlagen	x
1900113	Integritätscheck des Dateisystems fehlgeschlagen	x
1900114	Integritätscheck des Dateisystems fehlgeschlagen	x
1900115	Integritätscheck des Dateisystems fehlgeschlagen	x
1900204	Initialisierung des Watchdogs fehlgeschlagen	x
1900206	Initialisierung des Watchdogs fehlgeschlagen	x
1900303	Kritisches Kernellog erkannt	x
1900305	Datenpartition nicht korrekt gemounted	x
1900306	Systempartition nicht korrekt gemounted	x
1900307	Bootpartition gemounted	x
1900308	Überprüfung der Datenpartition fehlgeschlagen	x
1900309	Überprüfung der Systempartition fehlgeschlagen	x
1900501	Nicht alle benötigten Prozesse konnten gestartet werden	
1900103	Der Prozess x wurde zu häufig neugestartet	x
1900502	Der Selbsttest läuft bereits und kann nicht erneut ausgeführt werden	
1900504	Es wurde ein unerlaubt gestarteter Prozess gefunden	x
1900601	Es wurde ein Reboot aus unbekannten Gründen erkannt	
1900602	Es wurde ein Reboot wegen Wegfall der Versorgungspannung erkannt	
1900603	Es wurde ein unerwartetes Reboot-Kommando ausgeführt	
1900604	Es wurde ein Reboot durch den externen Watchdog erkannt	
1900605	Es wurde ein Reboot durch den internen Watchdog erkannt	
1900606	Es wurde ein Reboot durch einen Hardware-Reset erkannt	
600500	Das Gerät befindet sich im SLDM	
1900401	Der Watchdog kann einen Prozess nicht neustarten und führt daher einen Systemneustart durch	
1900301	Der Watchdog kann einen Prozess nicht neustarten und führt daher einen Systemneustart durch	
1600003	Kommunikation zum Sicherheitsmodul fehlgeschlagen. Führe Neustart aus.	
1600004	Selektieren des GWA AUTH-Schlüssels fehlgeschlagen	
1600025	Selektieren des EF zum initialen Import des Rootzertifikats fehlgeschlagen	
1600026	Speichern des initialen Rootzertifikats im Sicherheitsmodul fehlgeschlagen	
1600027	Aktivieren des initialen Rootzertifikats im Sicherheitsmodul fehlgeschlagen	
1600028	Das einzuspielende initiale Rootzertifikat basiert auf einer nicht erlaubten elliptischen Kurve	

Fehlercode	Beschreibung	Soft Lock-Down Modus
1600032	OID zu der elliptischen Kurve des initialen Rootzertifikats nicht gefunden	
1600033	Erstellen des Importzertifikats des initialen Rootzertifikats fehlgeschlagen	
1600034	Erstellen des Importzertifikats des initialen Rootzertifikats fehlgeschlagen	
1600035	Erstellen des Importzertifikats des initialen Rootzertifikats fehlgeschlagen	
1600037	Speichern des Public Key des initialen Rootzertifikats im Sicherheitsmodul fehlgeschlagen	
1600045	Aktualisieren des Import-Status des initialen Rootzertifikats fehlgeschlagen	
1600050	Selektieren des EF zum Import eines neuen Rootzertifikats fehlgeschlagen	
1600051	Speichern eines Rootzertifikats im Sicherheitsmodul fehlgeschlagen	
1600052	Aktivieren eines Rootzertifikats im Sicherheitsmodul fehlgeschlagen	
1600056	Wechsel in das DF SMGW im Sicherheitsmodul zum Import eines Rootzertifikats fehlgeschlagen	
1600058	Fehler während der Signaturerstellung durch das Sicherheitsmodul	
1600059	Import des Public Key eines Root-Zertifikats fehlgeschlagen	
1600062	Selektieren des EF zum Import eines Gütesiegelzertifikats fehlgeschlagen	
1600063	Speichern eines Gütesiegelzertifikats im Sicherheitsmodul fehlgeschlagen	
1600064	Aktivieren eines Gütesiegelzertifikats im Sicherheitsmodul fehlgeschlagen	
1600068	Fehler während der Signaturverifizierung	
1600069	Signatur ist ungültig	
1600079	Aktualisieren des Import-Status des initialen Rootzertifikats fehlgeschlagen	
1600080	Aktualisieren des Gütesiegel-Import-Status fehlgeschlagen	
1600086	Aktualisieren des LifeCycles im Sicherheitsmodul fehlgeschlagen	
1600101	Aktualisieren des Rootzertifikat-Import-Status fehlgeschlagen	
1600107	Konfigurieren des Subject und Issuer Namens fehlgeschlagen	
1600108	Intialisieren der Zertifikatsgenerierung fehlgeschlagen	
1600112	Konfigurieren der Zertifikatsvaliditätszeiträume fehlgeschlagen	
1600114	Konfigurieren der Seriennummer fehlgeschlagen	
1600115	Konfigurieren der Zertifikatsextensions fehlgeschlagen	
1600116	Erstellung des Zertifikats aus den Konfigurationoptionen fehlgeschlagen	
1600119	Speichern des neu erstellten Zertifikats fehlgeschlagen	
1600122	Beide WAN Schlüsselbänke sind belegt oder die zweite Bank wurde noch nicht erstellt	
1600123	Generieren der Schlüsselpaare im Sicherheitsmodul fehlgeschlagen	
1600125	Aktualisieren des Rootzertifikat-Import-Status fehlgeschlagen	
1600129	Speichern des neuen Zertifikats fehlgeschlagen	
1600132	Fehler während der Signaturverifizierung	
1600133	Signatur ist ungültig	
1600137	Das Format der AUTH Challenge Response Signatur ist ungültig	
1600138	Interner Fehler im Sicherheitsmodul beim Aktivieren des AUTH- Zustands	
1600140	Interner Fehler im Sicherheitsmodul beim Terminieren des AUTH-Zustands	
1600141	Abfragen einer AUTH Challenge vom Sicherheitsmodul fehlgeschlagen	
1600143	Bestimmung des verwendeten ECDSA Algorithmus fehlgeschlagen	
1600170	Fehler während der Überprüfung der SHA1 Routine	x
1600171	Fehler während der Überprüfung der MD5 Funktionalität	x
1600172	Fehler während der Überprüfung der SHA224/SHA256 Funktionalität	x
1600173	Fehler während der Überprüfung der SHA384/SHA512 Funktionalität	x

Fehlercode	Beschreibung	Soft Lock-Down Modus
1600174	Fehler während der Überprüfung der AES Funktionalität	x
1600175	Fehler während der Überprüfung der GCM Funktionalität	x
1600176	Fehler während der Überprüfung der CMAC Funktionalität	x
1600177	Fehler während der Überprüfung der Base64 Funktionalität	x
1600178	Fehler während der Überprüfung der Langzahlarithmetik Funktionalität	x
1600179	Fehler während der Überprüfung des Zufallsgenerators	x
1600189	Fehler während der Signaturerstellung durch das SMGW	
1600190	Fehler während der Überprüfung der elliptischen Kurven Funktionalität	x
1600194	Fehler während der Überprüfung der Entropy Funktionalität	x
1600196	Fehler während der Überprüfung des Zufallsgenerators	x
1600197	Aktivieren des neuen Zertifikats fehlgeschlagen	
1600198	Aktivieren der neuen Zertifikate fehlgeschlagen	
1600201	Fehler beim Deaktivieren von HAN-, WAN- oder LMN-Schlüssel	
1600211	Kommunikation zum Sicherheitsmodul fehlgeschlagen	
1600222	Fehler während der Überprüfung der Signaturverifizierungsfunktionalität	x
1600237	Der im Import-Zertifikat angegebene Key Slot ist belegt	
1600238	Verifikation des Link-Zertifikats mittels aktuellem Root-Zertifikat fehlgeschlagen	
1600244	Der Key Slot im Import-Zertifikat ist ungültig für ein Root-Zertifikat	
1600245	Um ein Root-Zertifikat zu löschen, müssen mindestens zwei Root-Zertifikate vorliegen	
1600246	Der PACE-Kanal zum Sicherheitsmodul kann nicht aufgebaut werden	
1600248	Löschen eines Root-Zertifikats im Sicherheitsmodul fehlgeschlagen	
1600250	Das zu löschende Root-Zertifikate wurde nicht gefunden	
1600255	Verbindung zum Sicherheitsmodul kann nicht aufgebaut werden	
1600257	Kommunikation zum Sicherheitsmodul fehlgeschlagen	
1600258	Interne Prozesskommunikation gestört	
1600268	Das einzuspielende Root-Zertifikat ist schon installiert	
1200508	Interne Prozesskommunikation gestört	
1200502	Interne Prozesskommunikation gestört	
1200503	Aktive SRV-Rolle (Erstkonfigurator, Servicetechniker) inkonsistent	x
1200504	Aktive SRV-Rolle ist weder Erstkonfigurator noch Servicetechniker	x
1200505	SRV-Server kann keine Anfragen entgegennehmen	
1200506	SRV-Server benutzt falschen Port	x
1200507	Zuviele SRV-Verbindungen zeitgleich offen	x
300018	Interne Prozesskommunikation gestört	
300019	Prozess für Messwertabfrage läuft nicht	
2500350	Integritätscheck der Datenbank ist fehlgeschlagen	x
2500351	Integritätscheck der Datenbank kann nicht ausgeführt werden	x
2500352	Integritätscheck der Datenbank ist fehlgeschlagen	x
2500353	Integritätscheck der Datenbank kann nicht ausgeführt werden	x
300033	Datenbankfehler: Messwert kann nicht in die originäre Messwertliste geschrieben werden	
300052	Datenbankfehler: Messwert kann nicht in die abgeleitete Messwertliste geschrieben werden	
300047	Das Gateway wurde noch nicht in die "normal operation" Phase überführt	
300067	Reinigungsprozess der MeterDB ist momentan aktiv	

Fehlercode	Beschreibung	Soft Lock-Down Modus
1500014	Verbindung zum GWA-NTPTLS-Server konnte nicht aufgebaut werden	
1500016	Timeout des internen ntpd	
1500021	Interner Fehler des ntpd	x
1500022	Interner Fehler des ntpd	x
1500042	GWA-NTPTLS-Kanal ist während der Synchronisation abgebrochen	
1500052	Interne Prozesskommunikation gestört	x
1500053	Interne Prozesskommunikation gestört	
1500054	Konfiguration des Zeitsystems ist nicht lesbar	x
1500055	Interne Prozesskommunikation gestört	
1500056	Abweichung bei Zeitsynchronisation zu groß	x
1500069	Es ist seit einem vorgegebenen Intervall keine Zeitsynchroinisation erfolgreich gewesen	x
1300116	Fehler der eigentlichen Installation während des Systemstarts	
1300405	TLS-Verbindung zum GWA abgebrochen oder beendet	
1300800	Integritätscheck eines Update-Pakets fehlgeschlagen	
1300801	Testinstallation eines Update-Pakets fehlgeschlagen	
1300804	Kompatibilitätscheck eines Update-Pakets zur aktuellen Firmware fehlgeschlagen	
1300160	Interne Prozesskommunikation gestört	
1300161	Fehler in internen Zustandsvariablen	
1300162	Fehler in internen Zustandsvariablen	
1300163	Fehler in internen Zustandsvariablen	
1300164	Fehler in internen Zustandsvariablen	
1300165	Fehler in internen Zustandsvariablen	
1300166	Fehler in internen Zustandsvariablen	
1300167	Fehler in internen Zustandsvariablen	
1300168	Fehler in internen Zustandsvariablen	
1000008	Interne Prozesskommunikation gestört	
1000009	Interne Prozesskommunikation gestört	
1000010	Interne Prozesskommunikation gestört	
1000011	Wake-Up Server kann keine Anfragen entgegennehmen	x
1000012	Wake-Up Server benutzt falschen Port	x
1000013	Wake-Up Server kann keine Anfragen entgegennehmen	x
2600101	Die Selbsttestfunktion vom lmnmanager konnte über IPC nicht aufgerufen werden	
2600102	Die Selbsttestfunktion vom wlmnmanager konnte über IPC nicht aufgerufen werden	
2600118	Die Selbsttestfunktion vom cls-proxy konnte über IPC nicht aufgerufen werden	
2600108	Die Selbsttestfunktion vom consumerinterface konnte über IPC nicht aufgerufen werden	
2600104	Die Selbsttestfunktion vom customeradministration konnte über IPC nicht aufgerufen werden	
2600105	Die Selbsttestfunktion vom gwaclient konnte über IPC nicht aufgerufen werden	
2600107	Die Selbsttestfunktion vom gwa-tls-client konnte über IPC nicht aufgerufen werden	
2600109	Die Selbsttestfunktion vom interfacemanager konnte über IPC nicht aufgerufen werden	
2600114	Die Selbsttestfunktion vom logsystem konnte über IPC nicht aufgerufen werden	

Fehlercode	Beschreibung	Soft Lock-Down Modus
2600117	Die Selbsttestfunktion vom mmc-diagnostic-read konnte über IPC nicht aufgerufen werden	
2600111	Die Selbsttestfunktion vom ntp-tls-proxy konnte über IPC nicht aufgerufen werden	
2600106	Die Selbsttestfunktion vom profilemanager konnte über IPC nicht aufgerufen werden	
2600116	Die Selbsttestfunktion vom secmodmanager konnte über IPC nicht aufgerufen werden	
2600112	Die Selbsttestfunktion vom srv-webserivce konnte über IPC nicht aufgerufen werden	
2600103	Die Selbsttestfunktion vom tariffmanager konnte über IPC nicht aufgerufen werden	
2600115	Die Selbsttestfunktion vom timesystem konnte über IPC nicht aufgerufen werden	
2600119	Die Selbsttestfunktion vom updatesystem konnte über IPC nicht aufgerufen werden	
2600110	Die Selbsttestfunktion vom wake-up service konnte über IPC nicht aufgerufen werden	

6.4 Konformitätserklärungen

*Die aktuelle DE-Konformitätserklärung finden Sie auf der Internetseite www.emh-metering.com im Bereich „**Produkte & Lösungen**“ bei der Produktbeschreibung zum CASA.*

*Die aktuelle EU-Konformitätserklärung finden Sie auf der Internetseite www.emh-metering.com im Bereich „**Produkte & Lösungen**“ bei der Produktbeschreibung zum CASA.*

6.5 Normen und Richtlinien

BSI-CC-PP-0073	Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.3
BSI-CC-PP-0077-V2-2015	Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.03
BSI-TR-03109	Technische Richtlinie „Dachdokument“, Version 1.1
BSI-TR-03109-1	Technische Richtlinie „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“, Version 1.1
BSI-TR-03109-1-Detailspezifikation	Technische Richtlinie „Detailspezifikation“, 2021-09-17
DIN VDE V 0418-63-10	Messeinrichtungen und -systeme – Teil 63-10: Logmeldungen und Ereignisse intelligenter Messsysteme
GPL	General Public License
IEC 60715	Abmessungen von Niederspannungsschaltanlagen und Geräten. Standardisierte Montage auf Schienen zur mechanischen Unterstützung elektrischer Geräte in Schalt- und Geräteanlagen

6.6 Abkürzungsverzeichnis

Basiszähler	⇔ Digitaler Stromzähler mit besserer Verbrauchsanzeige zur Integration in iMSys
BMWK	⇔ Bundesministerium für Wirtschaft und Klimaschutz
BSI	⇔ Bundesamt für Sicherheit in der Informationstechnik
CASA	⇔ Communication Access Security Administrator
CLS	⇔ Controllable Local System
CSV	⇔ Comma separated values
DHCP	⇔ Dynamic Host Configuration Protocol
DIN	⇔ Deutsches Institut für Normung e.V.
EMT	⇔ Externer Marktteilnehmer
EnWG	⇔ Energiewirtschaftsgesetz
FNN	⇔ Forum Netztechnik/Netzbetrieb im VDE
GPL	⇔ GNU General Public Licence
GPRS	⇔ General Packet Radio Service
GWA	⇔ Gateway-Administrator
HAN	⇔ Home Area Network
HDLC	⇔ High-Level Data Link Control
HEMS	⇔ Home Energy Management System
HTTP	⇔ Hypertext Transfer Protocol
HÜID	⇔ Herstellerübergreifende Identifikationsnummer
IEC	⇔ International Electrotechnical Commission
iMSys	⇔ intelligentes Messsystem
IPv4	⇔ Internet Protocol Version 4
IPv6	⇔ Internet Protocol Version 6
LED	⇔ Light-Emitting Diode (Leuchtdiode)
LMN	⇔ Local Metrological Network
LTE	⇔ Long Term Evolution
LV	⇔ Letztverbraucher
MSB	⇔ Messstellenbetreiber
OBIS	⇔ Object Identification System
OMS	⇔ Open Metering System
PIN	⇔ Personal Identification Number
PKI	⇔ Public Key Infrastructure
PTB	⇔ Physikalisch-technische Bundesanstalt
Root-CA	⇔ Root Certification Authority
SHA	⇔ Secure Hash
SIM	⇔ Subscriber Identity Module
SMGW	⇔ Smart Meter Gateway
ST	⇔ Servicetechniker
TAF	⇔ Tarifanwendungsfall
TLS	⇔ Transport Layer Security
TRuDI	⇔ Transparenz- und Display-Software der PTB
VDE	⇔ Verband der Elektrotechnik Elektronik Informationstechnik e. V.
WAN	⇔ Wide Area Network
WAN-A	⇔ Wide Area Network-Antenne
wM-Bus	⇔ Wireless M-Bus

EMH metering GmbH & Co. KG • Neu-Galliner Weg 1 • 19258 Gallin • GERMANY • Tel. +49 38851 326-0 • info@emh-metering.com • www.emh-metering.com