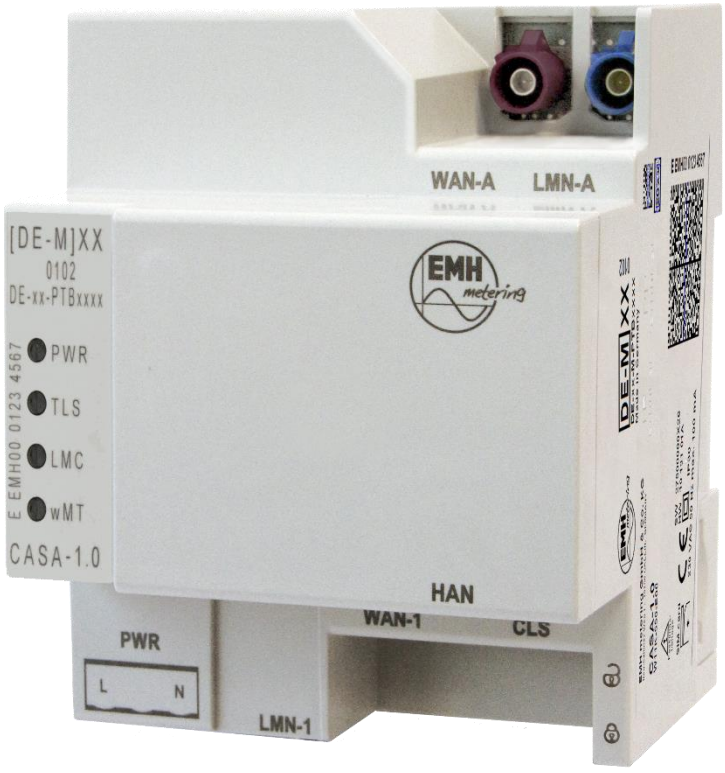
CASA 1.0 (CASA-AGD)

Benutzerhandbuch

für Letztverbraucher



DE Stand: 14.12.2019
CASA-PHB-LV-DE-1.17

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.

Der CASA enthält Open-Source-Komponenten. Nähere Informationen erhalten Sie auf Anfrage.

Bei Fragen oder Anregungen erreichen Sie uns unter:

EMH metering GmbH & Co. KG

Neu-Galliner Weg 1
19258 Gallin / DEUTSCHLAND

Tel.: +49 38851 326-0
Fax: +49 38851 326-1129

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

Einleitung

☞ Für den sicheren Umgang mit dem CASA ist es notwendig, dieses Dokument aufmerksam und vollständig zu lesen und zu beachten!

☞ In diesem Dokument werden Abkürzungen verwendet, die im Kapitel 9.6 „Abkürzungsverzeichnis“ / Seite 52 erläutert sind.

Hinweise zum CASA 1.0 - Benutzerhandbuch für Letztverbraucher

- Dieses Benutzerhandbuch ist Teil der Dokumentation des CASA. Es enthält die notwendigen Informationen zum sicheren Gebrauch. Lesen Sie diese Anleitung vor Beginn aller Arbeiten aufmerksam durch. So vermeiden Sie Personen- und Sachschäden. Bewahren Sie dieses Produkthandbuch sowie alle anderen mitgelieferten Unterlagen sorgfältig auf, damit sie während der gesamten Lebensdauer des Gerätes zur Verfügung stehen.

  Weitere Information zur Produktdokumentation beschreibt das Dokumentationskonzept / Seite V.

  Beachten Sie bei der Bedienung des CASA unbedingt auch alle Dokumente, die anderen Komponenten (z. B. Zählern) beiliegen.

Zielgruppe

- Dieses Benutzerhandbuch wendet sich an Letztverbraucher (LV).

Geltungsbereich

- In diesem Benutzerhandbuch sind alle Ausführungsvarianten und Funktionen des Gerätes beschrieben. Beachten Sie, dass diese Varianten in Bezug auf Konfiguration, Datenschnittstellen, Ein-/Ausgängen u. a. unterschiedlich ausgeführt sein können. Möglicherweise sind daher Merkmale beschrieben, die auf das von Ihnen eingesetzte Gerät nicht zutreffen.
- Die verfügbaren Ausführungsvarianten entnehmen Sie bitte den Datenblattangaben zum Gerät.
- Abbildungen in diesem Benutzerhandbuch dienen dem besseren Verständnis und können von der tatsächlichen Ausführung des Gerätes abweichen.

Bestimmungsgemäßer Gebrauch

- Der CASA ist ausschließlich für die Erfassung und Übertragung der Messdaten in Verbindung mit zugelassenen Messgeräten gemäß der technischen Beschreibung und nach ordnungsgemäßer Installation zu verwenden.
- Zum bestimmungsgemäßen Gebrauch gehört auch die Einhaltung aller Angaben in dieser Anleitung. Jede über den bestimmungsgemäßen Gebrauch hinausgehende Verwendung oder andersartige Benutzung gilt als Fehlgebrauch.

Wartungs- und Gewährleistungshinweise

Der CASA ist wartungsfrei. Bei Schäden (z. B. durch Transport, Lagerung) dürfen eigenständig keine Reparaturen vorgenommen werden. Beim Öffnen des Gerätes erlischt der Gewährleistungsanspruch. Gleiches gilt, 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.

§ Wurde das Sicherheitssiegel beschädigt oder entfernt, sind die Daten des CASA nicht mehr für die Abrechnung zugelassen und die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist erloschen.

Verwendete Symbole und Warnhinweise

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

Gefahr durch elektrische Spannung

„Gefahr durch elektrische Spannung“ kennzeichnet einen Warnhinweis, dessen Nichtbeachtung unmittelbar zu schweren Körperverletzungen oder zum Tod führt. Ergreifen Sie unbedingt alle geeigneten Maßnahmen zur Abwehr der Gefahr!

WARNUNG

„Warnung“ kennzeichnet einen Hinweis auf eine möglicherweise gefährliche Situation, die zu Körperverletzungen oder zu Sachbeschädigungen führen kann. Vermeiden Sie die gefährliche Situation!

ACHTUNG

Kennzeichnet einen Warnhinweis, dessen Nichtbeachtung zu Sachschäden führen kann.

HINWEIS

„Hinweis“ kennzeichnet wichtige Informationen im Handbuch.

ACHTUNG Funksender!

Der Funksender kann elektronische Geräte in ihrer Funktion beeinträchtigen! Mobilfunkverbot beachten!

Funktion

Kennzeichnet eine Funktionsbeschreibung des Gerätes.

Juristischer Hinweis

„Hinweis“ kennzeichnet wichtige Informationen im Handbuch.

Arbeitsschritt

Aktion erforderlich, z. B. *„Drücken einer Taste“* oder *„Eingabe eines Wertes“*

Tipp / Hinweis

Macht auf eine besondere Situation aufmerksam oder gibt einen Tipp zur Funktion

Hinweis GWA

Hinweis bzw. Anweisung speziell für den Gateway-Administrator (GWA)

Hinweis ST

Hinweis bzw. Anweisung speziell für den Service-Techniker (ST)

Hinweis MSB

Hinweis bzw. Anweisung speziell für den Messstellenbetreiber (MSB)

Hinweis LV

Hinweis bzw. Anweisung speziell für den Letztverbraucher (LV)

Dokumentationskonzept

Die Dokumentation zum CASA besteht aus mehreren Dokumenten, die nachfolgend benannt sind:

- Die Gebrauchsanleitung ist jedem Gerät beigelegt.
- Das Installations- und Konfigurationshandbuch ist für Service-Techniker (ST) und Gateway-Administratoren (GWA) und beschreibt den Umgang mit dem CASA und seinen Komponenten von der Installation bis zur Entsorgung sowie die Inbetriebnahme, Konfiguration und Wartung des CASA.
- Das Benutzerhandbuch für den Letztverbraucher (LV) enthält alle Informationen, die für die Nutzung eines bereits installierten und in Betrieb genommenen CASA erforderlich sind.
- Hinweise zur Prüfung der Integrität liegen im Kapitel 1.3 „Integritätssicherung der Dokumentation“ / Seite 9 vor.

Dokumentation zu diesem Produkt und Versionen

Benennung	Handbuch
CASA 1.0 – Installations- und Konfigurationshandbuch für Service-Techniker und für Gateway-Administratoren	CASA-PHB-ST-GWA-DE
CASA 1.0 – Benutzerhandbuch für Letztverbraucher	CASA-PHB-LV-DE
CASA 1.0 – SMGw-Schnittstellenbeschreibung (CASA API)	CASA-API

Tabelle 1: Übersicht der Dokumente

Dokumentation im Internet auf:
http://www.emh-metering.com
Zu finden unter „**Produkte & Lösungen**“ und „**Smart Meter Gateway**“ - **CASA**

Historie

Version	Datum	Erstellt von:	Status	Beschreibung
Rev. 1.04	01.11.2018	MLP, JPL	Bearbeitung	Initialisierung des Dokuments UR-Dokument TR CASA
Rev. 1.04.01	20.11.2018	RGI	Bearbeitung	Anpassung der Übersicht über die „Aufteilung der einzelnen Kapitel auf die drei Produkthandbücher“
Rev. 1.05 a	15.02.2019	JPL	Bearbeitung	Layout-Anpassungen Änderungen vom Observation Report (OR) TüViT (OR_AGD_v3) übernommen
Rev. 1.06	10.10.2019	JPL, MGO	Bearbeitung	Änderungen aufgrund Observation Report ORv4.
Rev. 1.07	31.10.2019	MGO	Bearbeitung	Kap. 2.2 um Hardware-Versionen zu Ersatz-bauteilen erweitert
Rev. 1.08	08.11.2019	MGO	Bearbeitung	Inhalte des Kap. 1.4 durch einen Verweis auf das betreffende separate Dokument ersetzt
Rev. 1.09	13.11.2019	MGO	Bearbeitung	Kap. 1.4 zu mess- und eichrechtskonformer Verwendung entfernt. Kap. 2.2 entsprechend Observation Report ORv11 ALC angepasst und Software-Version hinzugefügt. Kap. 9.3.7 aktualisiert.
Rev. 1.10	14.11.2019	MGO	Bearbeitung	Kap. 1.3 überarbeitet und um Hinweise auf Security-Target-Dokument ergänzt
Rev. 1.11	18.11.2019	MGO	Bearbeitung	Dokument umbenannt: „CASA…“ → „CASA 1.0…“ Abschnitt zum Dokumentationskonzept um CASA-API-Dokument erweitert Kap. 7.4 überarbeitet entsprechend Observation Report ORv5 AGD Kap. 9.4 aktualisiert
Rev. 1.12	20.11.2019	MGO	Bearbeitung	Symbole und Warnhinweise überarbeitet für ORv5
Rev. 1.13	21.11.2019	MGO	Bearbeitung	überarbeitet für ORv5
Rev. 1.14	22.11.2019	MGO	Bearbeitung	überarbeitet für ORv6
Rev. 1.15	27.11.2019	MGO	Bearbeitung	Kap. 2.2: Beschreibung zur Gerätebeschriftung überarbeitet, Software-Versionsnummer angepasst Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.16	12.12.2019	MGO	Bearbeitung	Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.17	14.12.2019	MGO	Bearbeitung	Kap. 3.2.2, 3.2.3 und 3.2.4 zur Darstellung des Sicherheitssiegels überarbeitet Kap. 9.5: Dokumentenreferenzen aktualisiert

Inhaltsverzeichnis

1 Allgemeine Sicherheitshinweise

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

1.1 Sicherheitshinweise

Befolgen Sie unbedingt folgende Hinweise:

- Lesen Sie alle beiliegenden Anleitungen und Informationen.
- Beachten Sie die Warnungen am Gerät und in den Dokumenten.
- Verwenden Sie das Gerät nur in technisch einwandfreiem Zustand und ausschließlich im Sinne der bestimmungsgemäßen Verwendung.
- Der CASA darf nicht außerhalb der spezifizierten technischen Daten betrieben werden (siehe Leistungsschild und Kapitel 2.6 „Technische Daten“ / Seite 18).
- Führen Sie die Bedienung am Gerät stets sicherheits- und gefahrenbewusst aus.
- Beachten Sie die Wartungs- und Gewährleistungshinweise (siehe „Wartungs- und Gewährleistungshinweise“ / Seite III).
- Im vorliegenden Dokument beziehen sich die gegebenen konkreten Informationen oder Handlungsanweisungen zum CASA immer auf einen autorisierten Benutzer, d.h.,
    - den autorisierten Gateway-Administrator (GWA),
    - den autorisierten Service-Techniker (ST),
    - den autorisierten Letztverbraucher (LV),
    - den autorisierten Messstellenbetreiber (MSB),
    - den autorisierten externen Marktteilnehmer (EMT),

  auch wenn im Text die Rollenbezeichnung ohne den Zusatz „autorisiert“ angegeben ist.

1.2 Maßnahmen und Sicherheitsziele

Um die Sicherheitsziele des CASA zu erfüllen, müssen folgende Maßnahmen getroffen werden:

Sind die nachfolgend benannten Bedingungen nicht eingehalten, darf der CASA nicht verwendet werden.

Der CASA soll in einer nichtöffentlichen Umgebung in den Räumlichkeiten des Letztverbrauchers (LV) installiert werden. Der Installationsort muss mit einem Grundniveau an physischem Schutz ausgestattet sein. Der Schutz beinhaltet den CASA und den Zähler, die mit dem CASA kommunizieren.
Nur autorisierte Personen dürfen physischen Zugang zum CASA haben.

1.3 Integritätssicherung der Dokumentation

Zur Absicherung gegen nicht autorisierte Modifikationen der Dokumente auf den Webseiten der EMH metering GmbH & Co. KG sind für die Dokumente kryptografische Prüfsummen nach dem Secure Hash Algorithm „SHA256“ hinterlegt.

Der Begriff Secure Hash Algorithm (kurz SHA, englisch für sicherer Hash-Algorithmus) bezeichnet eine Gruppe standardisierter kryptografischer Hashfunktionen. Diese dienen zur Berechnung eines Prüfwerts (Hash-Wert) für Daten und Dokumente.

Diese Hash-Werte können von jedem Nutzer der Handbücher verwendet werden, um die Integrität der Handbücher zu überprüfen.

Die Hash-Werte für die Benutzerdokumente zum CASA sind im Dokument „CASA 1.0 Security Target (CASA-ST)“ geführt, das Bestandteil des Common-Criteria-Zertifizierungsverfahrens mit der ID BSI-DSC-CC-0919 beim Bundesamt für Sicherheit in der Informationstechnik (BSI) ist.
Das Security-Target-Dokument kann von den Webseiten des BSI heruntergeladen werden.

Ein Download-Link zum aktuellen Stand des Security-Target-Dokuments ist unter https://www.emh-metering.com/ im Bereich „**Produkte & Lösungen**“ zur Produktbeschreibung des Smart Meter Gateway hinterlegt.

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 Web-Seite 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 über das Kontextmenü im Windows-Explorer mit der rechten Maustaste auf die Datei, zu dem der Hash-Wert erzeugt werden soll, ausgewählt werden.
- Als Ergebnis wird eine Datei „sha256.txt“ erzeugt, in der der Hash-Wert enthalten ist.
- Der erzeugte Hash-Wert muss mit dem auf der 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

Der CASA ist eine eichpflichtige Zusatzeinrichtung für intelligente Messsysteme.

- Der CASA ist eine Kommunikationseinheit mit Zulassung durch die Physikalisch-Technische Bundesanstalt (PTB) und Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Hardware- und Softwarekomponenten sind so kombiniert und konfiguriert, dass alle Zählerdaten den Anforderungen (z.B. nach Lieferantenvertrag) gemäß registriert, gespeichert und an die Zentrale des Messstellenbetreibers (MSB) bzw. eines externen Marktteilnehmers (EMT) (z. B.: eines Energieversorgungsunternehmens) weitergeleitet und somit für Messdatenbereitstellung sowie Abrechnungszwecke verfügbar sind. Zudem sichert der CASA die Kommunikationsverbindungen zwischen steuerbaren Geräten (z. B. zur Steuerung dezentraler Erzeuger und flexibler Lasten) und externen Marktteilnehmern (EMT).
- Der CASA erhält von verschiedenen Zählern (z. B.: Strom, Gas, Wasser, Wärme…) deren gemessene Zählerstände. Nach den Vorgaben des Versorgungsvertrages des Letztverbrauchers (LV) mit dem Energieversorgungs-unternehmen werden die Messwerte gesammelt, signiert und gespeichert, um anschließend über eine Wide Area Network-Schnittstelle (WAN) an berechtigte Marktteilnehmer versendet zu werden. Auf diese Weise erhält beispielsweise der Versorger die Daten zur Abrechnung. Des Weiteren können Letztverbraucher (LV) über die Home Area Network-Schnittstelle (HAN) Verbrauchsdaten bzw. Service-Techniker (ST) Systeminformationen abrufen.

2.2 Beschriftung des Gerätes

Frontansicht

Seitenansicht von rechts

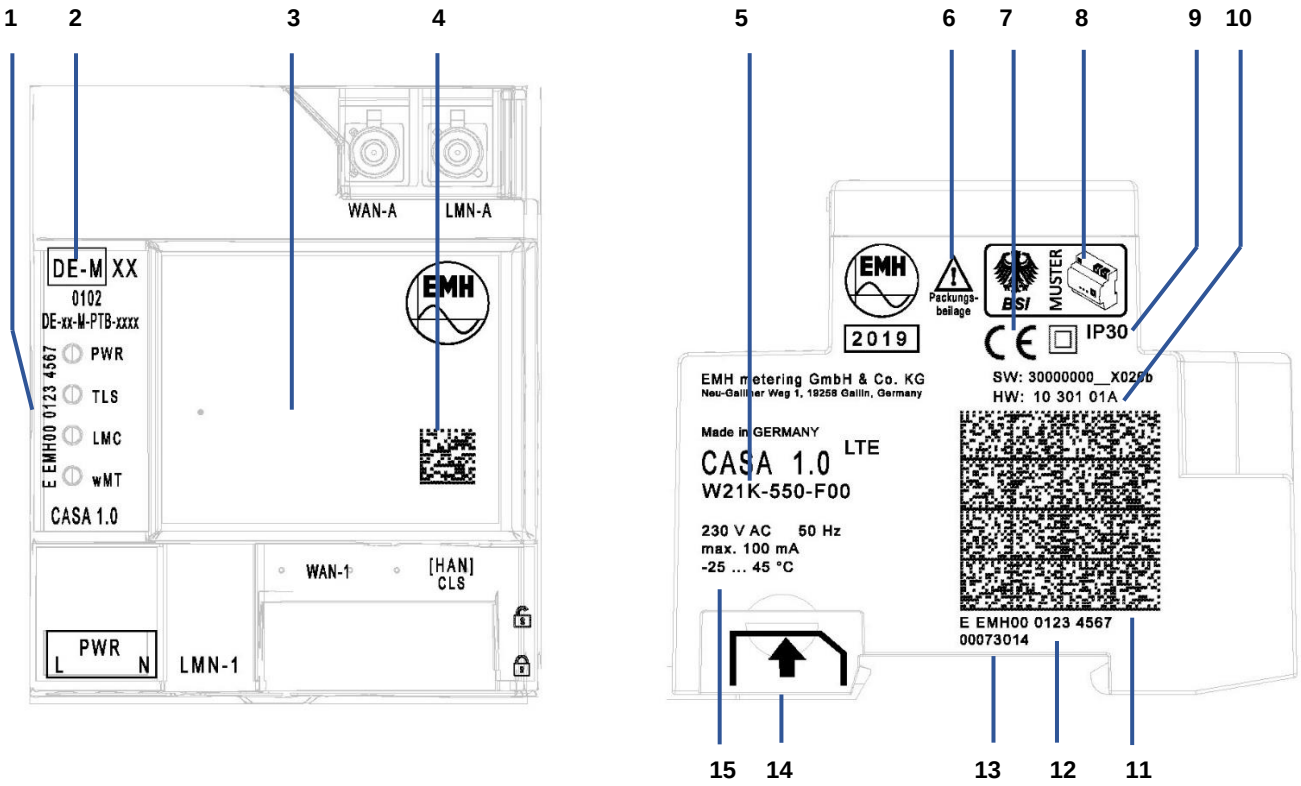


Abbildung 1: Frontansicht und Seitenansicht von rechts

1	Herstellerübergreifende Identifikationsnummer (HÜID)
2	Konformitätskennzeichnung und Nummer der Baumusterprüfbescheinigung der PTB (Die in Abbildung 1 mit „X“ oder „x“ gekennzeichneten Stellen sind auf dem ausgelieferten Gerät durch die Jahresangabe und Zulassungsnummer ersetzt.)
3	Platz für Eigentumsbeschriftung
4	Data Matrix Code des Eigentümers (bei Bedarf)

5	Typenbezeichnung und Typenschlüssel
6	Hinweis auf Packungsbeilage
7	CE-Kennzeichnung
8	Zertifizierungszeichen des BSI (Die in Abbildung 1 mit „MUSTER“ gekennzeichnete Stelle ist auf dem ausgelieferten Gerät durch die Zertifizierungsnummer ersetzt.)
9	Schutzart und Schutzklasse
10	SW: Software-Version (zum Zeitpunkt der Herstellung): 30000000__X026b HW: Hardware-Version[1], mögliche Hardware-Versionen bei Verwendung von funktionsgleichen Alternativbauteilen: 10 301 xxx 10 302 xxx 10 303 xxx 10 304 xxx
11	Data Matrix Code
12	Herstellerübergreifende Identifikation (HÜID)
13	Seriennummer des Sicherheitssiegels
14	Abbildung zur Installation der SIM-Karte
15	Spannung, Frequenz, Stromaufnahme und Temperaturbereich

[1] Die Hardware-Version beschreibt in den ersten fünf Stellen den Hardware-Stand des zertifizierungsrelevanten Teils des CASA (Ziffern „10 301“ in Abbildung 1). Die Bauteile des CASA, die nicht Bestandteil der Zertifizierung nach Common Criteria sind, werden in den letzten drei Stellen der Hardware-Versionsnummer dokumentiert (Ziffern „01A“ in Abbildung 1).

2.3 Gehäuse- und Anzeigeelemente

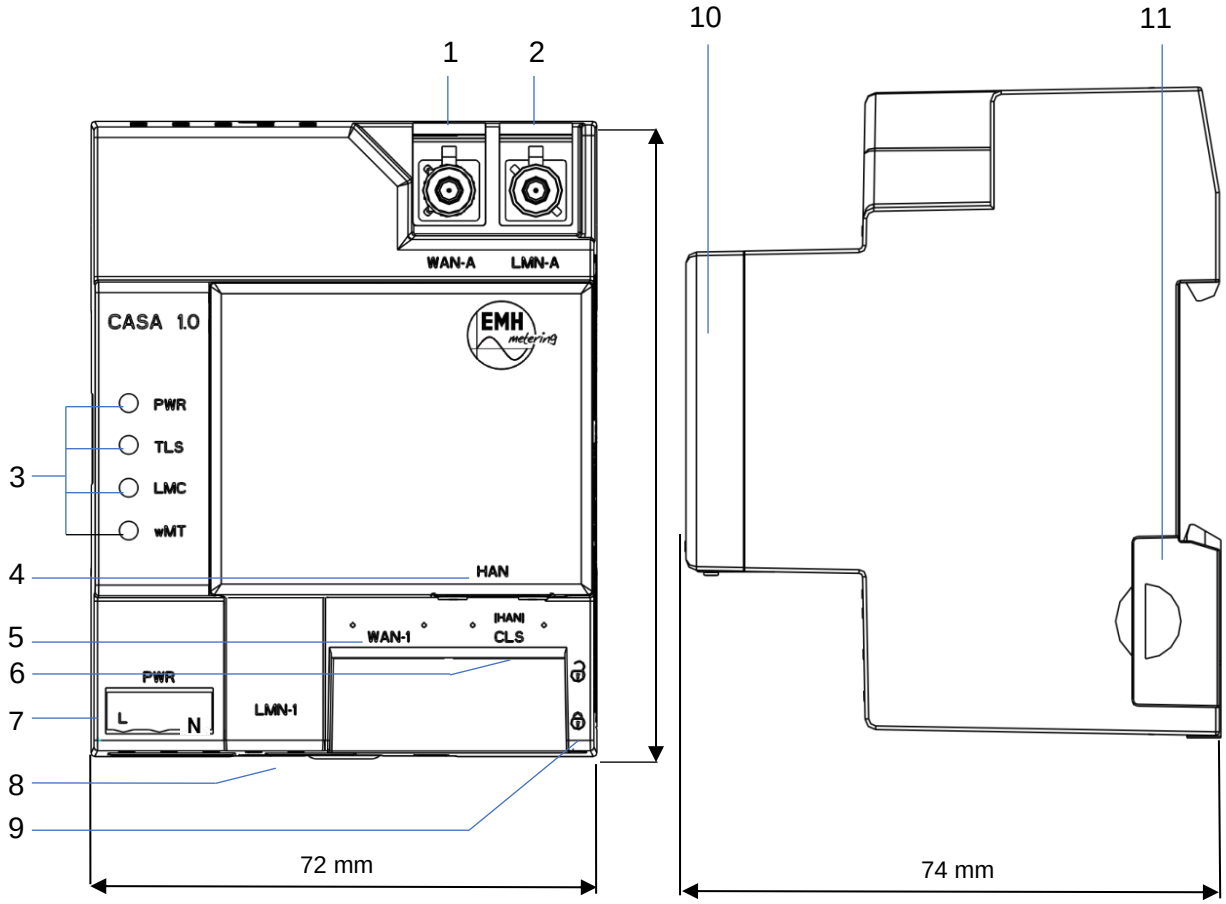


Abbildung 2: Frontansicht (links) Seitenansicht von rechts (rechts)

1	WAN-Antennenanschluss (WAN-A), FAKRA-D-Stecker
2	Wireless M-Bus-Antennenanschluss (LMN-A), FAKRA-C-Stecker
3	LEDs (siehe Kapitel 2.3.2 „LEDs an der Frontseite“ / Seite 15)
4	HAN-Schnittstelle RJ45
5	WAN-1-Schnittstelle RJ45
6	[HAN] CLS-Schnittstelle RJ45
7	Anschluss für Betriebsspannung 230 V (PWR)
8	LMN-1-Schnittstelle RJ12-RS485
9	Verriegelung für Mehrwertmodul
10	Mehrwertmodul (HAN)
11	SIM-Karten Slot

2.3.1 CASA mit HAN-Modul

Der CASA mit Mehrwertmodul im betriebsfähigen Zustand ist in der Abbildung 3 / Seite 14 dargestellt.

Abbildung 3: Gehäuse mit HAN-Modul

2.3.2 LEDs an der Frontseite

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

LED	Bedeutung	Beschreibung
PWR (grün)	Power	**Aus** solange die Initialisierung der Firmware läuft. **Blinkt** bei Abschluss der Initialisierung. Die Dienste der Firmware werden nun gestartet. **Leuchtet dauerhaft**, wenn die physische Betriebsbereitschaft hergestellt ist, d.h. alle Dienste der Firmware gestartet und betriebsbereit sind. **Heartbeat** (zweimal schnell blinken, lange Pause), wenn sich das Gerät im Soft-Lock-Down-Mode (siehe auch dazu Kapitel 8 „Fehlerbehebung“ / Seite 38) befindet und durch einen Gateway-Administrator (GWA) kontrolliert werden muss.
TLS (grün)	Transport Layer Security	**Blinkt** ab Beginn des Aufbaus des TLS-Kanals. **Leuchtet dauerhaft**, wenn die TLS-Verbindung zum Gateway-Administrator (GWA) mittels eines Wirkzertifikats erfolgt ist (Normalbetrieb). **Blinkt**, wenn die TLS-Verbindung zum Gateway-Administrator (GWA) mittels eines Gütesiegelzertifikats erfolgt ist. **Aus**, wenn die Verbindung zum Gateway-Administrator (GWA) getrennt wurde.
LMC (grün)	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.
wMT (blau)	Wireless MBus Traffic	**Leuchtet kurz auf**, wenn ein Wireless-MBus-Datensatz empfangen wird.
PWR, TLS, LMC, wMT	Hard-Lock-Down-Mode	**Es blinken alle 4 LEDs dauerhaft,** wenn sich das Gerät im Hard-Lock-Down Mode (siehe auch dazu Kapitel 8 „Fehlerbehebung“ / Seite 38) befindet und getauscht werden muss.

Tabelle 2: LEDs am CASA

2.3.3 LEDs an den Schnittstellen

LED	Bedeutung	Beschreibung
Ethernet an → HAN-Schnittstelle → [HAN] CLS Schnittstelle → WAN-Schnittstelle	Physikalischer Ethernet-Anschluss	**Leuchtet dauerhaft grün**, zeigt erkannte Verbindung zu Ethernet-Gerät (i.d.R. Switch oder Router). **gelb, blinkt** beim Empfang oder Senden von Ethernet-Paketen über physikalische Verbindung.

Tabelle 3: LEDs an den Schnittstellen

Die LEDs dienen ausschließlich zur Erkennung der korrekten Installation durch den Service-Techniker (SV) vor Ort bzw. unterstützen bei der Fehlersuche.

Die LEDs müssen für den Letztverbraucher (LV) nicht zwingend sichtbar sein und sind ggf. durch Abdeckungen verdeckt.

2.4 Funktionen des CASA

2.4.1 Messwerte für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung

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

Im Folgenden wird die Messwertverarbeitung für bestimmte Anwendungszwecke, wie der Tarifierung von Verbrauchs- und Einspeisemengen sowie für die Erhebung von Netzzustandsdaten durch den CASA beschrieben. Dabei erhebt der CASA auch Messdaten, die von Netzbetreibern u. a. für die Bilanzierung von Energienetzen verwendet werden.

2.4.2 Anwendungsfälle

In diesem Kapitel werden die Anwendungsfälle für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung beschrieben, die der CASA erfüllen kann.

- Der externe Marktteilnehmer (EMT) erhält bei jedem Anwendungsfall die Messwertliste vom CASA.
- Zähler und Messwertgrößen werden über die Geräte-IDs der Zähler und die OBIS-Kennzahlen der zu erfassenden Messgrößen ausgewählt. Der CASA versieht die Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur. Zu einem per Konfiguration festgelegten Zeitpunkt wird die Messwertliste dann an die berechtigten Marktteilnehmer versendet.
- Ein Gültigkeitszeitraum legt fest, ab welchem Zeitpunkt das Regelwerk für einen Anwendungsfall in Kraft treten soll und zu welchem Zeitpunkt es wieder deaktiviert wird.

TAF1 – Datensparsame Tarife nach § 40(5) EnWG

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 (LV) gemacht werden können. Es wird nur eine Tarifstufe betrachtet. Es ist jedoch möglich, die Zählerstände mehrerer Zähler eines Letztverbrauchers (LV) zu addieren bzw. zu subtrahieren und als Gesamtverbrauch bzw. -einspeisung zu versenden. 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 ist dabei vom Gateway-Administrator (GWA) nicht kürzer als 1 Monat zu wählen.

TAF2 – Zeitvariable Tarife nach § 40(5) EnWG

Bei diesem Anwendungsfall stellt der Lieferant dem Letztverbraucher (LV) für unterschiedliche Zeiträume verschiedene Preise für die in den jeweiligen Zeiträumen registrierten Energiemengen in Rechnung. Hierzu werden im CASA mehrere Tarifstufen definiert, an die jeweils eine Zeitbedingung geknüpft ist. Die Zeitbedingungen der Tarifstufen werden wiederum über Tarifschaltzeitpunkte definiert. Zu jedem Zeitpunkt ist jeweils nur eine Tarifstufe aktiv.
Zum Tarifumschaltzeitpunkt erfasst der CASA die Zählerstände von einem oder mehreren Zählern. Der CASA erzeugt einen Eintrag in der Messwertliste und fügt die angefallene Energiemenge zwischen den beiden letzten Umschaltzeitpunkten der zuletzt gültigen Tarifstufe hinzu.

TAF6 – Abruf von Messwerten im Bedarfsfall

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

- dem Ein- und Auszug eines Letztverbrauchers (LV),
- bei einem Wechsel des Lieferanten oder
- dem Wechsel in den Grundversorgungstarif.

Damit auch 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 wieder aus der Messwertliste gelöscht.

Die Daten werden im begründeten Ausnahmefall im Auftrag eines externen Marktteilnehmers (EMT) durch den Gateway-Administrator (GWA) ausgelesen und zu einem Stichtag an den externen Marktteilnehmer (EMT) weitergeleitet.

TAF7 – Zählerstandsgangmessung

Dieser Anwendungsfall erlaubt die Erfassung und den Versand von Zählerstandsgängen. Über diesen Anwendungsfall 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.

TAF10 – Abruf von Netzzustandsdaten

Um Netzbetreibern zu ermöglichen, den Zustand ihrer Netze zu beurteilen, können im CASA Netzzustandsdaten bzw. Statusinformationen der angeschlossenen Zähler bereitgestellt werden. Diese Daten können dann periodisch oder bei Eintritt bestimmter Ereignisse an die berechtigten externen Marktteilnehmer (EMT) versendet werden. Der CASA unterstützt in diesem Zusammenhang die folgenden Ereignisse zum Auslösen des Datenversands:

- Veranlassung durch den Gateway-Administrator (GWA),
- ein Messwert überschreitet einen bestimmten Schwellenwert,
- ein Messwert unterschreitet einen bestimmten Schwellenwert

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

Die Tarifanwendungsfälle TAF3 bis TAF5, TAF8, TAF9 und TAF11 bis TAF 14 werden vom CASA aktuell nicht unterstützt.

2.5 Firmware-Update

- Der CASA ist ein IT-System, welches einer stetigen Weiterentwicklung unterliegt. Neben technischen Weiterentwicklungen werden regelmäßig Sicherheitsupdates automatisch durchgeführt. Diese werden durch kryptografische Signaturfunktionen vor Manipulation und Übertragungsfehlern geschützt. Das Firmware-Update wird durch den Gateway-Administrator (GWA) durchgeführt.

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

2.6 Technische Daten

Versorgung	Spannung Strom Frequenz	230 V AC max. 100 mA 50 Hz
Echtzeituhr	Gangreserve	48 h
Anzeigen	4 LEDs	Anzeigen für: PWR (Power), TLS (Transport Layer Security), LMC (Local Meter Controller), wMT (Wireless-MBus-Traffic)
Geräteschnittstellen	Zählerschnittstellen Kundenschnittstellen Weitbereichsschnittstellen	LMN-1, LMN-A HAN, [HAN] CLS WAN-1, WAN-A
Sicherheit/EMV	Sicherheit Störfestigkeit Störaussendung	EN 60950-1, 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 DIN EN 50470-1, Kap. 6.2, Tabelle 9
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 Polycarbonat glasfaserverstärkt, halogenfrei, recyclebar gemäß IEC 62052-11, Kunststoffe gemäß UL94V-0
Umgebungs-bedingungen	mechanische elektromagnetische vorgesehener Einsatzort	M1 gemäß Messgeräterichtlinie (2014/32/EU) E2 gemäß Messgeräterichtlinie (2014/32/EU) Innenraum gemäß EN 50470-1
Gewicht		ca. 200 g
LMN-1 RS485	Ausgangsspannung Strombelastbarkeit RS485 Geschwindigkeit Anschluss	12 V DC +/-5% max. 290 mA 921,6 kBit/s 6P6C-Buchse (RJ12)
LMN-A Wireless M-Bus	Wireless M-Bus Anschluss	S-Mode oder T-/C-Mode (gemäß EN 13757-4 und nach BSI TR-03109-1 Anlage III) 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-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)
WAN-A (Lösung 1) GSM/GPRS	Frequenzbereiche GPRS Anschluss	Quadband GSM850 (850 MHz) / E-GSM (900 MHz) / DCS (1800 MHz) / PCS (1900 MHz) Klasse 10 FAKRA-Stecker, D-codiert, bordeaux-violett
WAN-A (Lösung 2) LTE	Frequenzbereiche GPRS/LTE Anschluss	LTE-Modul (Fallback EDGE/GPRS), Triband (Band 3 / 1800 MHz; Band 8 / 900Hz; Band 20 / 800 MHz) Klasse 10 FAKRA-Stecker, D-codiert, bordeaux-violett

Tabelle 4: Technische Daten

3 Sicherheit

3.1 Prüfung der Integrität

Die Integrität des CASA muss vor der Montage und Inbetriebnahme durch den Service-Techniker (ST) überprüft werden. Dazu werden die äußeren Sicherheitsmerkmale am Gerät geprüft.

Das Sicherheitssiegel muss auf seine Unversehrtheit überprüft werden. Die Darstellungen für unbeschädigte Siegel und beschädigte Siegel entnehmen Sie Kapitel 3.2 „CASA Sicherheitssiegel“ / Seite 20.

Werden Beschädigungen am Gehäuse oder am Sicherheitssiegel des CASA festgestellt, darf das Gerät nicht verwendet werden.

In diesem Fall informieren Sie bitte Ihren Messstellenbetreiber (MSB).

3.2 CASA Sicherheitssiegel

3.2.1 Position des Sicherheitssiegels

In der nachfolgenden Abbildung sehen Sie die Fläche für das Aufbringen des Siegels. Im Detail sind die korrekt zusammengeführten Gehäusekanten zu erkennen, welche im Herstellungsprozess mit dem Sicherheitssiegel beklebt werden. Auf diese Weise wird das nicht autorisierte Öffnen des Gehäuses erkennbar gemacht.

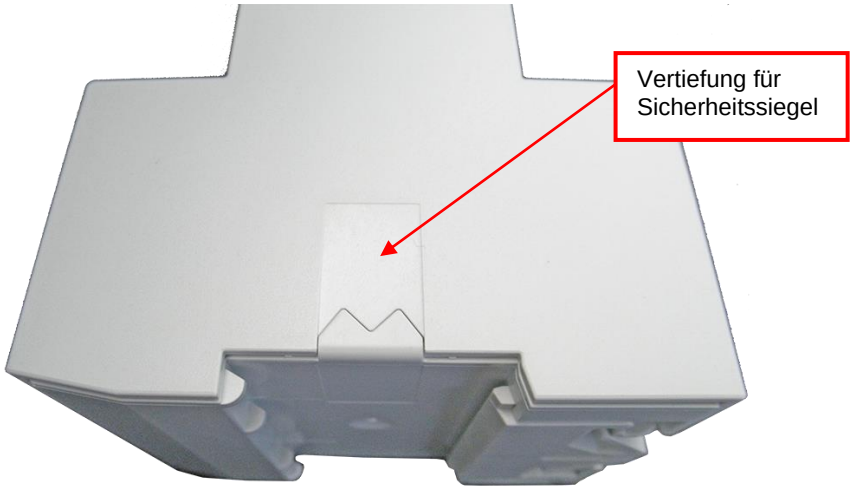


Abbildung 4: Vertiefung für die Position des Sicherheitssiegels

3.2.2 EMH Sicherheitssiegel

Die Gesamtansicht des Siegels bei Beleuchtung mit Tageslicht und seine Abmessungen zeigt Abbildung 5.

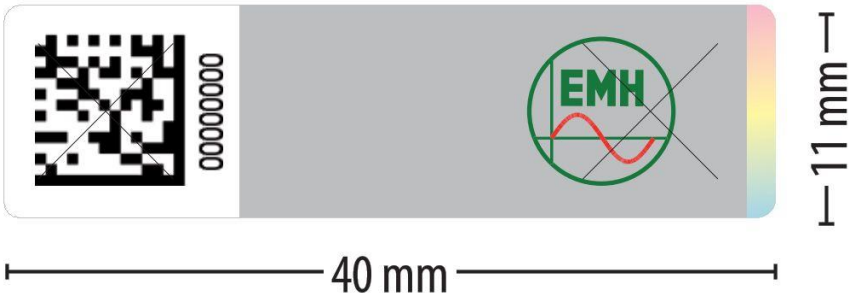
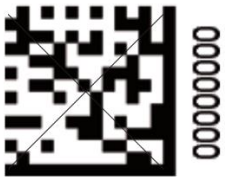


Abbildung 5: Gesamtansicht des Sicherheitssiegels

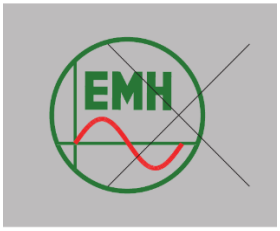
Bei Beleuchtung mit UV-Licht wird das gelb-grünlich leuchtende Sicherheitsmerkmal des Siegels wie in Abbildung 6 dargestellt erkennbar.

Abbildung 6: Ansicht des Sicherheitssiegel unter UV-Licht

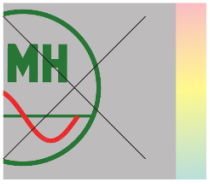
Weitere Sicherheitsmerkmale des Sicherheitssiegels im Detail zeigt die nachfolgende Abbildung 7.



Jedes Siegel ist mit einer eindeutigen Seriennummer gekennzeichnet. Die Seriennummer ist sowohl in lesbarer Form als auch in einem Data Matrix Code aufgedruckt.
Die Seriennummer des Siegels ist ebenfalls im Typenschild des CASA an der Gehäuseseite angegeben.
(siehe Kapitel 2.2 „Beschriftung des Gerätes“ / Seite 12)



Das Siegel verfügt über zwei Sicherheitsstanzungen: eine im EMH-Logo (siehe links) und eine im Data Matrix Code (siehe oben).



Das Siegel verfügt über ein optisches Echtheitsmerkmal, das je nach Lichteinfall einen Verlauf des gesamten sichtbaren Farbspektrums zeigt.

Abbildung 7: Sicherheitsmerkmale des Sicherheitssiegels

3.2.3 Unbeschädigte Sicherheitssiegel

In der nachfolgenden Tabelle 5 sehen Sie Beispiele für unbeschädigte und korrekt positionierte Siegel.

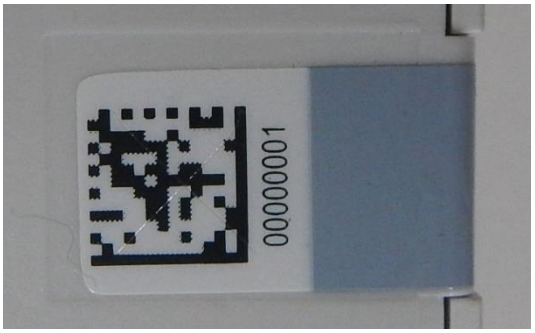
Unbeschädigte Siegel	Beschreibung
	korrektes Siegel
	korrektes Siegel
	korrektes Siegel

Tabelle 5: Beispiele für korrekte Siegel

3.2.4 Beschädigte Sicherheitssiegel

In der nachfolgenden Tabelle 6 sehen Sie Beispiele für beschädigte Siegel.

Werden Beschädigungen am Gerät oder am Sicherheitssiegel festgestellt, darf das Gerät nicht verwendet werden.

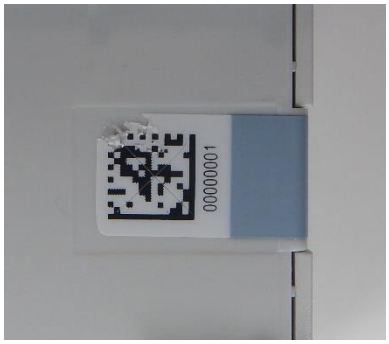
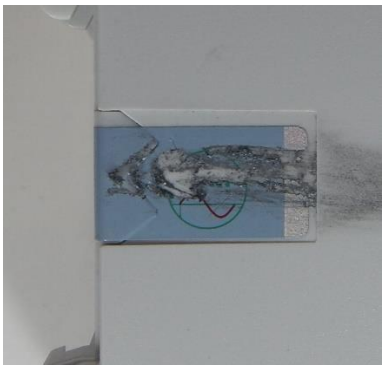
Beschädigte Sicherheitssiegel	Beschreibung
	zerstörtes Sicherheitssiegel nach mechanischem Manipulationsversuch ✗
	zerstörtes Sicherheitssiegel nach mechanischem Manipulationsversuch ✗
	zerstörtes Sicherheitssiegel nach Manipulationsversuch mit chemischen Lösemitteln ✗
	zerstörtes Sicherheitssiegel nach mechanischem Manipulations-versuch mit Kälteeinwirkung ✗
	zerstörtes Sicherheitssiegel nach Manipulationsversuch mit Wärmeeinwirkung ✗

Tabelle 6: Beispiele für beschädigte Sicherheitssiegel

4 Kommunikation

4.1 Externe Kommunikationswege des CASA

Der CASA stellt Schnittstellen in die folgenden drei Netzbereiche zur Kommunikation bereit:

- **LMN** (Local Metrological Network)
  In diesem Netzwerk übertragen die angebundenen Zähler für Strom, Gas, Wasser oder Wärme eines oder mehrerer Letztverbraucher (LV) ihre Messdaten an den CASA.
- **WAN** (Wide Area Network)
  Im WAN kommuniziert der CASA mit dem Gateway-Administrator (GWA) und externen Marktteilnehmern (EMT). Zur Anbindung an das WAN stellt der CASA zwei physikalische Schnittstellen bereit:
- **HAN (**Home Area Network**)**
  Über die HAN-Schnittstelle hat der Letztverbraucher (LV) die Möglichkeit die ihm zugeordneten Informationen abzurufen.
- **[HAN]** CLS-Schnittstelle (Home Area Network - CLS)

  Über den [HAN] CLS-Anschluss kommuniziert der CASA mit Controllabe Local Systems (CLS) des Letztverbrauchers (LV), wie z. B. Kraft-Wärme-Kopplungs- oder Photovoltaik-Anlagen und Stromunterbrechern. Gesteuert wird diese Kommunikation durch externe Marktteilnehmer (EMT) im WAN.

  Die Verbindung zwischen externen Marktteilnehmern (EMT) im WAN und den Controllabe Local Systems (CLS) im HAN wird durch eine Proxy-Komponente im CASA hergestellt.

4.2 Interne Kommunikation und Sicherheitskonzept des CASA

4.2.1 Software Sicherheitskonzept

- Die Software des CASA beinhaltet zahlreiche Mechanismen zur Absicherung des Systems sowohl gegen zufällige und unabsichtliche Informationsveränderungen als auch gegen gezielte Manipulation und zur Vermeidung von Bedienfehlern durch Gateway-Administratoren (GWA), Service-Techniker (ST) oder Letztverbraucher (LV).
- Entsprechend der sicherheitstechnischen Vorgaben 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 in der Kommunikation mit dem Gateway-Administrator (GWA) verwendeten Zertifikate sind auf einen Vertrauensanker in der Root-CA (Root Certificate Authority) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zurückzuführen.

4.2.2 Schutz der gespeicherten Messwerte gegen Verfälschung

- Es ist nicht möglich, die im CASA gespeicherten Messwerte durch Zugriff über eine der Geräteschnittstellen zu verändern. Siehe hierzu auch Kapitel 6 „Rollen und Zugriffsberechtigungen“ / Seite 29.
- Die Daten sind zudem mit einer digitalen Signatur versehen, die eine unbemerkte Verfälschung der Daten ausschließt.

4.2.3 Schutz des Programmcodes

Der CASA führt eine automatische, zyklische Prüfung der eichpflichtigen Software im Langzeitspeicher durch. Diese Prüfung wird sowohl regelmäßig durch den CASA als auch auf Anfrage durch den Gateway-Administrator (GWA) oder den Letztverbraucher (LV) durchgeführt und verifiziert die Signaturen der installierten Software. Dadurch kann

eine zufällige Informationsverfälschung oder Manipulation im Langzeitspeicher durch physikalische Effekte zuverlässig erkannt werden.

4.2.4 Schutz von übertragenen und gespeicherten Daten

Die eichpflichtige Software fasst die zu einem Messzeitpunkt erfassten eichtechnisch relevanten Informationen eines Zählers zu einem Zählerdatensatz zusammen, der digital signiert wird.
Diese digitale Signatur wird vor der Langzeitspeicherung der Datensätze angebracht. Somit können von einem empfangenden Gerät Verfälschungen an den Datensätzen durch Signaturprüfung erkannt werden, unabhängig davon, ob die Verfälschung auf den Datenspeicher oder während der Datenfernübertragung erfolgt sind.

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

Der CASA führt eine automatische zyklische Prüfung der Messwerte im Langzeitspeicher durch. Diese Prüfung wird sowohl regelmäßig als auch auf Anfrage des Gateway-Administrators (GWA) oder des Letztverbrauchers (LV) durchgeführt und verifiziert die Signaturen der gespeicherten Daten. Dadurch kann eine zufällige Informationsverfälschung im Langzeitspeicher auf Grund physikalischer Effekte zuverlässig erkannt werden.

4.2.5 Fehlererkennung der Zählerdaten

Die folgenden Fehlerfälle werden vom CASA erkannt:

- dauerhaft ausbleibender Empfang von Zählerdaten
- wiederholt auftretende Transportfehler
- 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 (GWA) gesendet.

4.3 Kommunikationsprotokolle

Zur Sicherung der Kommunikationswege von und zum CASA wird das Transport-Layer-Security-Protokoll (TLS) in der Ver. 1.2 eingesetzt.
Beim Aufbau jeder TLS-Verbindung wird die Authentizität der der Kommunikationspartner anhand wechselseitig ausgetauschter Zertifikate geprüft.

4.4 Inhaltsdatensicherung und Signaturbildung

Da für externe Marktteilnehmer (EMT) bestimmte Zähler-Daten gegebenenfalls vom CASA über den Gateway-Administrator (GWA) übertragen werden, ist der Dateninhalt für den zugehörigen externen Marktteilnehmer (EMT) verschlüsselt und Message Authentication Code (MAC)-gesichert sowie für die zugehörigen externen Marktteilnehmer (EMT) gekennzeichnet.
Darüber hinaus verschlüsselt der CASA seine lokalen Daten während der Speicherung in einem persistenten Speicher.

4.5 Pseudonymisierung von Daten

Die Netzzustandsdaten werden vor der Übertragung an den externen Marktteilnehmer (EMT) oder den Gateway-Administrator (GWA) pseudonymisiert. Auf diese Weise wird verhindert, dass der Empfänger die Daten einem Letztverbraucher (LV) zuordnen kann.

Die Pseudonymisierung von Netzzustandsdaten bei der Übertragung vom CASA an einen externen Marktteilnehmer (EMT) 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 (EMT) oder an den Gateway-Administrator (GWA) übertragen.
- Der Gateway-Administrator (GWA) prüft die Signatur der CASA und damit die Authentizität der Daten und leitet diese nach Entfernung der CASA-Signatur an den Empfänger weiter.
- Der Empfänger entschlüsselt die Daten.

5 Logbücher

5.1 Logbücher allgemein

Der CASA protokolliert seine Aktionen in drei unterschiedlichen Arten von Logbüchern:

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

☞ Die Zugriffsmöglichkeiten auf diese Logmeldungen bestehen gemäß folgender Tabelle:

Log	Zugriff	Schnittstelle
Letztverbraucher-Log	lesender Zugriff durch den Letztverbraucher (LV)	[HAN] und [HAN] CLS-Schnittstelle
System-Log	lesender Zugriff durch den Gateway-Administrator (GWA)	WAN-Schnittstelle
	lesender Zugriff durch den Service-Techniker (ST)	HAN-Schnittstelle
Eich-Log	lesender Zugriff durch den Gateway-Administrator (GWA)	WAN-Schnittstelle

Tabelle 7: Erlaubte Zugriffe auf die Logmeldungen

Jeder Logbucheintrag setzt sich aus den folgenden Informationen zusammen:

- Einem Zeitstempel,
- Einer eindeutigen Logbuchmeldung-Identifikationsnummer, die das eingetretene Ereignis beschreibt,
- Der digitalen Signatur (dies gilt nur für das Eich-Log).

5.2 Letztverbraucher-Log

Beachten Sie, dass niemand die Ereignisse löschen oder bearbeiten kann, die im Letztverbraucher-Log aufgezeichnet werden. Die Speicherdauer kann durch den Gateway-Administrator (GWA) konfiguriert werden, beträgt aber mindestens 15 Monate.

Ein Letztverbraucher (LV) hat Zugriff auf das Letztverbraucher-Log, wenn er die entsprechenden Zugangsdaten für die Authentifizierung von seinem Messstellenbetreiber (MSB) 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 dem Gateway-Administrator (GWA) der Zugriff auf das Logbuch Letztverbraucher-Log nicht gestattet.

Die Informationen des Letztverbraucher-Logs werden für den autorisierten Letztverbraucher (LV) vom CASA derart aufbereitet, dass er sie mit einem Webbrowser an der HAN-Schnittstelle ohne weitere Hilfsmittel lesen kann.

☞ Eine Liste der im Letztverbraucher-Log protokollierten Ereignisse finden Sie im Anhang in Kapitel 9.3 „Protokollierte Ereignisse“ / Seite 39.

5.3 System-Log

Der Zweck des Systems-Logs ist es, den Gateway-Administrator (GWA) und den autorisierten Service-Techniker (ST) über den Systemstatus der CASA zu informieren. Daher protokolliert der CASA in diesem Log jedes wichtige Ereignis (z. B. Fehlermeldungen, Ausfall der WAN-Verbindung, sicherheitsrelevante Ereignisse, Aktivitäten des Gateway-Administrators (GWA), etc.). Es werden keine datenschutzrelevanten Informationen (z. B. Zähler-Daten oder Messwerte) im System-Log gespeichert.

5.4 Eich-Log

Im Eich-Log werden eichtechnisch relevante Ereignisse (z. B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) beständig und nachvollziehbar gespeichert. Außerdem erfolgt die Registrierung von Änderungen an eichtechnisch relevanten Parametern (z. B. Zeitsprünge bei der Uhrzeitsynchronisation oder Änderungen der Tarifprofile). Jeder Eintrag in diesem Logbuch ist durch eine digitale Signatur mit dem privaten Signaturschlüssel des CASA vor nachträglicher absichtlicher oder unbeabsichtigter Verfälschung geschützt.

6 Rollen und Zugriffsberechtigungen

☞ **Der CASA arbeitet nach folgendem Rollenkonzept:**

6.1 Gateway-Administrator (GWA)

Der Gateway-Administrator (GWA) ist derjenige, der den CASA in Betrieb nimmt, konfiguriert, überwacht und steuert. Er erstellt und administriert die im CASA eingespielten Tarifprofile und führt bei Bedarf die Aktualisierung der Software des CASA durch. Für jeden einzelnen CASA gibt es nur einen Gateway-Administrator (GWA).

6.2 Service-Techniker (ST)

Der Service-Techniker (ST) kann die mit HAN und [HAN] CLS gekennzeichneten Anschlüsse nutzen, um z. B. das Logbuch „System-Log“ zur Diagnose von Fehlersituationen einzusehen (siehe Kapitel 5.3 „System-Log“ / Seite 28). Hierbei ist ausschließlich ein lesender Zugriff auf die anzuzeigenden Daten möglich.

6.3 Letztverbraucher (LV)

Letztverbraucher (LV) sind natürliche oder juristische Personen, die Energie für den eigenen Verbrauch oder Betrieb von Ladepunkten zur Versorgung von Elektrofahrzeugen beziehen. Der Letztverbraucher (LV) ist Eigentümer der im CASA verarbeiteten und gespeicherten Messwerte. Unter die Rolle des Letztverbrauchers fallen somit der Anschlussnutzer, ggf. der Anschlussnehmer und der Anlagenbetreiber.

Ein Letztverbraucher (LV) kann im Normalbetrieb des CASA folgende, nur ihn betreffende, Informationen einsehen:

- Messwertlisten,
- aktuelle und vergangene Verbrauchs- und/oder Einspeisewerte und
- das Logbuch Letztverbraucher-Log

Ein Letztverbraucher (LV) kann im Normalbetrieb folgende Funktionen ausführen:

- Ausführen des Selbsttests

Der Letztverbraucher (LV) kann keine Daten einsehen, die andere Letztverbraucher (LV) betreffen.

6.4 Externe Marktteilnehmer (EMT)

Externe Marktteilnehmer sind alle Teilnehmer mit Ausnahme des Gateway-Administrators (GWA), mit denen der CASA eine WAN-Kommunikation zum Austausch von Daten aufnehmen kann. Autorisierte und authentifizierte externe Marktteilnehmer (EMT), die private oder abrechnungsrelevante Daten erhalten, müssen vertrauenswürdig sein und dürfen keine unautorisierten Auswertungen dieser Daten mit Bezug auf den Verbraucher durchführen. Die Authentifizierung des externen Marktteilnehmers (EMT) erfolgt bei jedem Verbindungsaufbau.

Externe Marktteilnehmer (EMT) haben keinen schreibenden Zugriff auf den CASA und können auch keine Daten aktiv auslesen. Die einzige Übertragungsart ist Datenversand zum externen Marktteilnehmer (EMT), der stets vom CASA ausgeht.

6.5 Messstellenbetreiber (MSB)

Der Messtellenbetreiber (MSB) ist für die Messstelle und auch für deren Einrichtung verantwortlich. Er nimmt den vom Hersteller gelieferten CASA entgegen und beauftragt einen Service-Techniker (ST) mit der Montage des Gerätes an der betreffenden Messstelle.
Weiterhin ist der Messstellenbetreiber (MSB) für die ordnungsgemäße Inbetriebnahme und den Betrieb des CASA verantwortlich. Ein Gateway-Administrator (GWA) führt diese Aufgaben im Auftrag des Messtellenbetreibers durch.
Der Messstellenbetreiber (MSB) wird die von den Zählern erzeugten und vom CASA weitergeleiteten Messdaten über den Gateway-Administrator (GWA) erhalten und gegenüber dem Letztverbraucher (LV) abrechnen.

Der Messstellenbetreiber (MSB) hat keinen direkten Zugriff auf den CASA. Er bedient sich stattdessen des von ihm beauftragten Service-Technikers (ST) und des Gateway-Administrators (GWA).

6.6 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 die folgenden Merkmale für jeden Nutzer:

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

Der Authentifizierungsprozess erfolgt in der Regel während des TLS-Handshakes beim Aufbau eines TLS-Kanals. Hier werden je nach Rolle Client- oder Server-Zertifikate ausgetauscht, die dann vom CASA mit den im Gerät hinterlegten Zertifikaten verglichen werden (siehe 4.2.1 „Software Sicherheitskonzept“ / Seite 24). Dadurch kann die Gegenstelle genau einem Profil zugeordnet werden und damit 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 entsprechend konfiguriert werden.

7 Der Letztverbraucher (LV)

7.1 Rolle des Letztverbrauchers (LV)

Der CASA besitzt die Möglichkeit, die Mess- und Logdaten für den Letztverbraucher (LV) darzustellen. Diese Darstellung dient der Information für den Letztverbraucher.
(siehe Kapitel 7.3 „Letztverbraucher-Logbuch auslesen“ / Seite 34)

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

Ihre Zugangsdaten, die Sie für den Zugriff auf Ihre Daten im CASA benötigen, erhalten Sie von Ihrem Messstellenbetreiber (MSB). Bei diesen Zugangsdaten handelt es sich um:

- die HAN-IP-Adresse des CASA,
- Benutzernamen und Passwort oder das TLS-Zertifikat

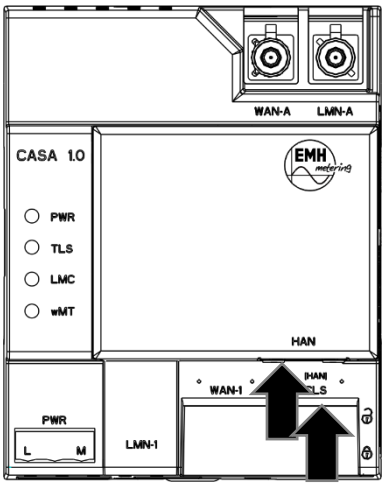
Die Authentifikationsgeheimnisse wie die bereitgestellte PIN, Benutzername, Zertifikats- und Schlüsselmaterial sind für Dritte unzugänglich aufzubewahren bzw. abzulegen. Die HAN-IP-Adresse des CASA kann durch den Gateway-Administrator (GWA) an Ihr Netzwerk angepasst werden.

Die für die Nutzung der Schnittstelle des Letztverbrauchers (LV) erforderlichen Parameter auf der Ebene des HTTPS-Protokolls sind im Detail im CASA-API-Dokument im Kapitel 8 beschrieben (siehe auch Kapitel 9.5 „Normen und Richtlinien“ / Seite 51).

Bei fehlerhaften Eingaben werden vom CASA Fehler als HTTP-Statuscodes zurückgemeldet. In diesem Fall korrigieren Sie bitte Ihre Eingabe.
Die möglichen Statuscodes sind im CASA-API-Dokument im Kapitel 8.4 beschrieben.

7.2 Kommunikationsverbindung einrichten

Um Ihre Zählerdaten einzusehen, gehen Sie wie folgt vor:



Schließen Sie Ihr Auslesegerät
- an die mit HAN gekennzeichnete Schnittstelle
  oder
- an die mit HAN-CLS gekennzeichnete Schnittstelle
  oder
- an die von Ihrem Messstellenbetreiber (MSB) anderweitig bereitgestellte HAN-Schnittstelle

des CASA an. Dazu wird ein abgeschirmtes Netzwerkkabel benötigt.

1. Stecken Sie das Netzwerkkabel in die betreffende RJ45-Ethernet-Buchse, bis der Stecker einrastet.
2. Das andere Ende des Kabels stecken Sie in die Netzwerk-anschlussbuchse Ihres Laptops oder PCs.

Das Auslesegerät und das benötigte Netzwerkkabel gehören nicht zum Lieferumfang des CASA.

Auf dem Auslesegerät muss ein Internet Browser installiert sein.
Der eingesetzte Internet Browser muss verschlüsselte Verbindungen mit dem TLS-Protokoll der Version 1.2 unterstützen.

3. Öffnen Sie den Internet Browser auf Ihrem PC und geben Sie in die Adressleiste des Browsers die HAN-IP-Adresse wie folgt ein:

https:// ← Ergänzen um IP-Adresse der HAN-Schnittstelle des CASA

4. Wählen Sie anschließend die Authentifizierungsmethode:

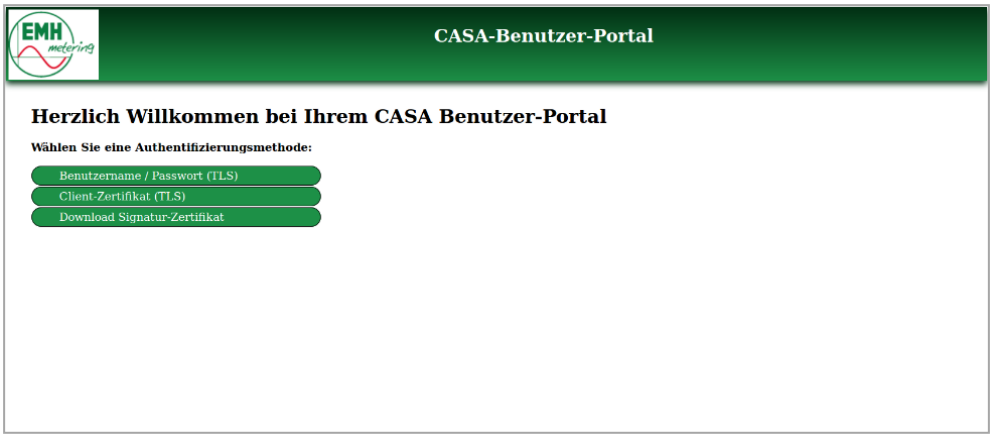


Abbildung 8: Beispiel für das CASA Benutzer-Portal

5. Authentifizieren Sie sich entweder mit der vom Gateway-Administrator (GWA) übermittelten Benutzername-Passwort-Kombination oder Ihrem TLS-Zertifikat.

▶ Es öffnet sich die Startseite des **CASA-Benutzer-Portals.**

Alternativ können Sie durch Auswahl der Schaltfläche „Download Signatur-Zertifikat“ das Signaturzertifikat des CASA[1] herunterladen, das zur Signaturprüfung der Messwerte benötigt wird.

Der CASA überwacht und beschränkt die Anzahl erfolgloser Anmeldeversuche.

Der voreingestellte Standardwert für die maximal zulässige Anzahl erfolgloser Anmeldeversuche ist auf 5 gesetzt.

Dieser Wert kann vom Gateway-Administrator (GWA)auf einen Wert zwischen 3 und 10 geändert werden.

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 (LV) bezieht sich auf den gesamten Letztverbraucherzugang.

Bei Fragen hierzu, wenden Sie sich bitte an Ihren Messstellenbetreiber (MSB).

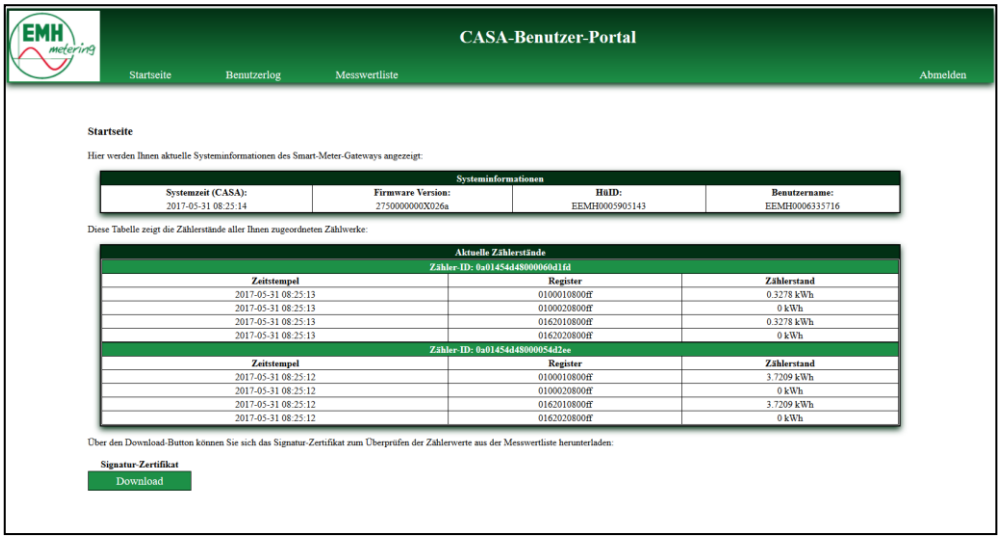


Abbildung 9: Beispiel für die Startseite des CASA-Benutzer-Portals

Der obere Navigationsbereich der Webseite gliedert sich in die Teilbereiche **Startseite**, **Letztverbraucher-Log** und **Messwertliste**. Außerdem befindet sich im Navigationsbereich ein „**Abmelden"-Button**, mit dessen Hilfe Sie sich ausloggen können. Ein automatisches Abmelden erfolgt nach 10-minütiger Inaktivität**.**

Zum Vor- und Zurücknavigieren nutzen Sie bitte die Funktionen Ihres Browsers.

Auf der **Startseite** finden Sie allgemeine Statusinformationen über den CASA und Ihre am CASA angeschlossenen Zähler. Zu diesen Informationen gehören:

- Die aktuelle Systemzeit des CASA.
- Die Systeminformationen des CASA.
- Die aktuellen Zählerstände.
- Der Download-Link für das Signatur-Zertifikat des CASA[1].
- Ein Button zum Auslösen eines Selbsttests.

[1] Mit dem Signatur-Zertifikat kann die Signatur von Messwerten überprüft werden. Wie die Daten zur Signatur-Prüfung im JSON-Format ausgelesen werden können, ist in Kapitel 8.3.2 des CASA-API-Dokuments beschrieben.

7.3 Letztverbraucher-Logbuch auslesen

Um Ihr Letztverbraucher-Log einzusehen und auszulesen gehen, Sie wie folgt vor:

- ▶ Wählen Sie „**Benutzer Logbuch“** im Navigationsbereich.
- ▶ Wählen Sie den gewünschten Zeitbereich.

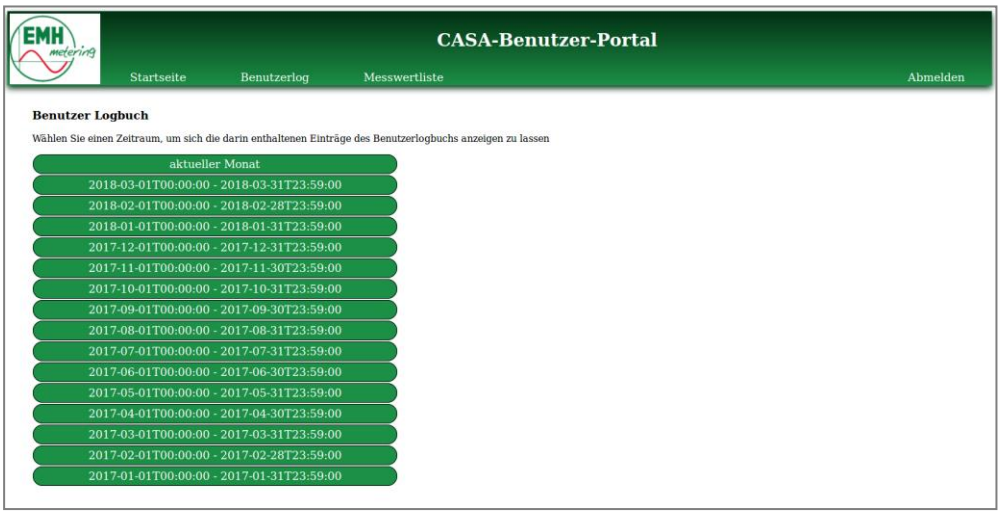


Abbildung 10: Beispiel für ein Benutzer Logbuch

- ▶ Es öffnet sich eine Seite mit einer tabellarischen Darstellung der des Letztverbraucher-Logs.

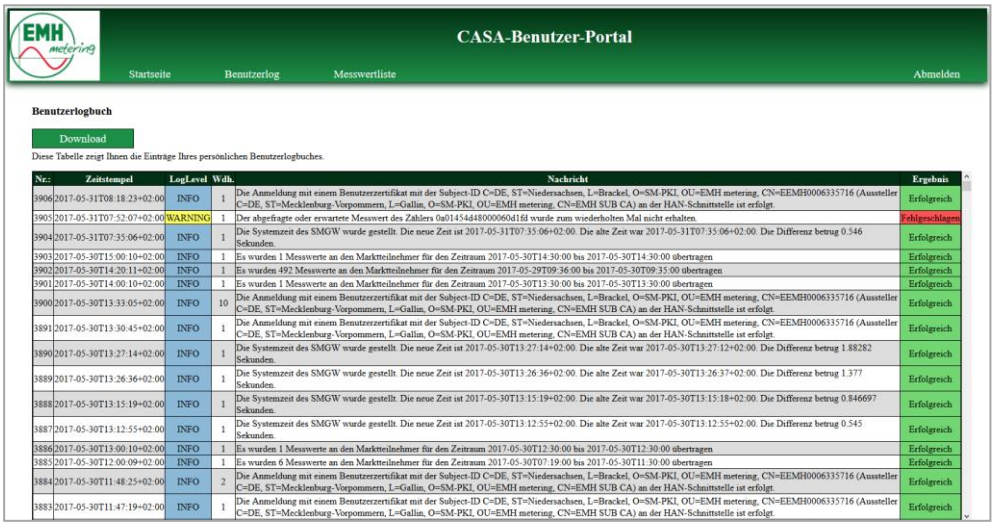


Abbildung 11: Beispielhafte Darstellung für Letztverbraucher-Log

Das Letztverbraucher-Log zeigt alle Ereignisse an, die entweder eichtechnisch relevant sind (z. B. Neustarts des Gateways, Uhrsynchronisation, veränderte Tarifprofile) oder den Datenfluss der dem Nutzer zugeordneten Daten beschreiben, wie z. B. den Versand von Messdaten an externe Marktteilnehmer.

Um das Letztverbraucher-Log im CSV-Format herunter zu laden, gehen Sie wie folgt vor:

- ▶ Klicken Sie auf Download.
- ▶ Speichern Sie die Datei.

Wie Sie die CSV-Datei in Ihren Texteditor, Ihr Tabellenkalkulationsprogramm oder Ihre Datenbank importieren, entnehmen Sie bitte der Beschreibung der jeweiligen Software.

7.4 Selbsttest auslösen

Der Selbstest des CASAs kann über den Button Auslösen auf der Startseite ausgeführt werden:

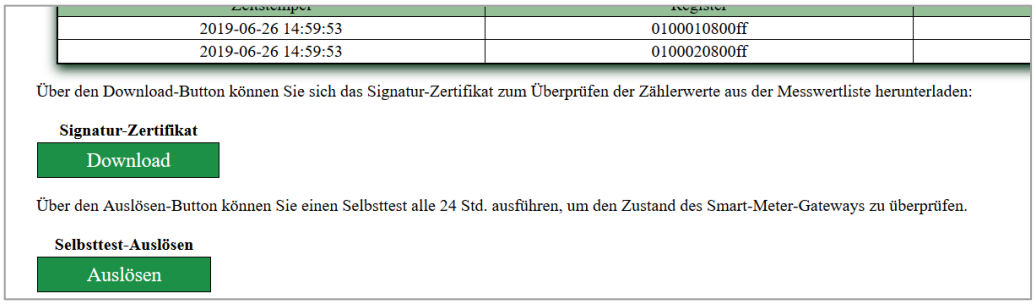


Abbildung 12: Ausführung eines Selbsttests

Der Selbsttest des CASA kann vom Letztverbraucher bei Bedarf ausgeführt werden, um die korrekte Funktion des Gerätes zu überprüfen.

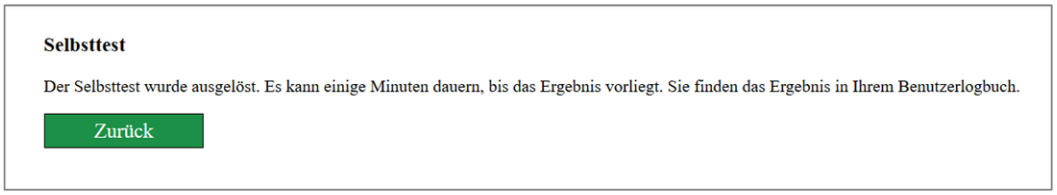


Abbildung 13: Anzeige nach Start des Selbsttests

Um eine übermäßige Belastung des CASA zu vermeiden, kann der Selbstest nur einmal alle 24 Stunden über die Web-Oberfläche ausgelöst werden. In allen anderen Fällen wird ein entsprechender Hinweistext ausgegeben.

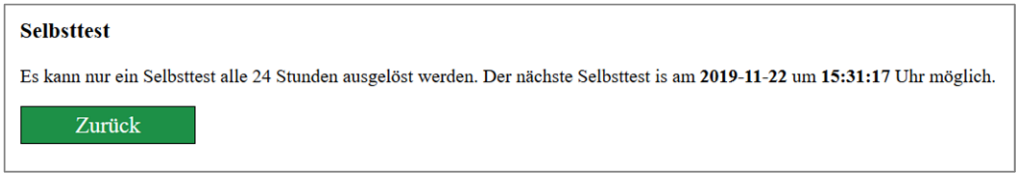


Abbildung 14: Fehlermeldung bei zu häufigem Start des Selbsttests

Sobald der Selbsttest beenden wurde, kann das Ergebnis über das Letztverbraucher-Log abgerufen werden.

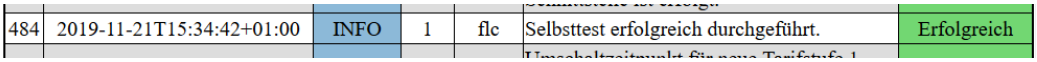


Abbildung 15: Beispiel eines Log-Eintrags bei erfolgreichem Selbsttest

Einige der im Zuge des Selbsttest möglichen Fehler versetzen den CASA in den Soft-Lock-Down-Modus (siehe Kapitel 8 „Fehlerbehebung“ / Seite 38). In diesem Fall kann das Ergebnis des Selbsttests über die Web-Oberfläche erst abgerufen werden, nachdem der Fehler vom Gateway-Administrator (GWA) behoben wurde. Die betreffenden Fehler sind im Kapitel 9.4 „Herstellerspezifische Fehlercodes“ / Seite 42 gesondert gekennzeichnet.

7.5 Messwertlisten auslesen

Um die Zählerdaten eines bestimmten Abrechnungszeitraums anzuzeigen und diese auszulesen, gehen Sie wie folgt vor:

1. Wählen Sie die **Messwertliste** im Navigationsbereich.
   ▶ Es öffnet sich eine Seite mit einer Liste aller Ihnen zugeordneten Tarifanwendungsfälle (TAF).

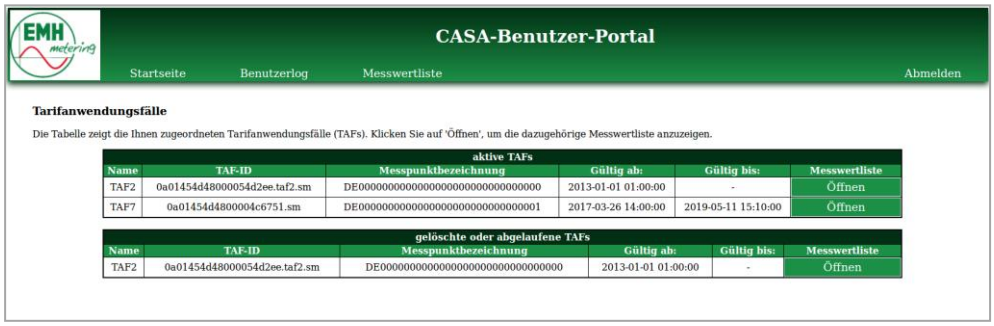


Abbildung 16: Beispielhafte Darstellung der vorhandenen Tarifanwendungsfälle (TAF)

1. Wählen Sie den gewünschten TAF aus und klicken Sie auf **Öffnen**.

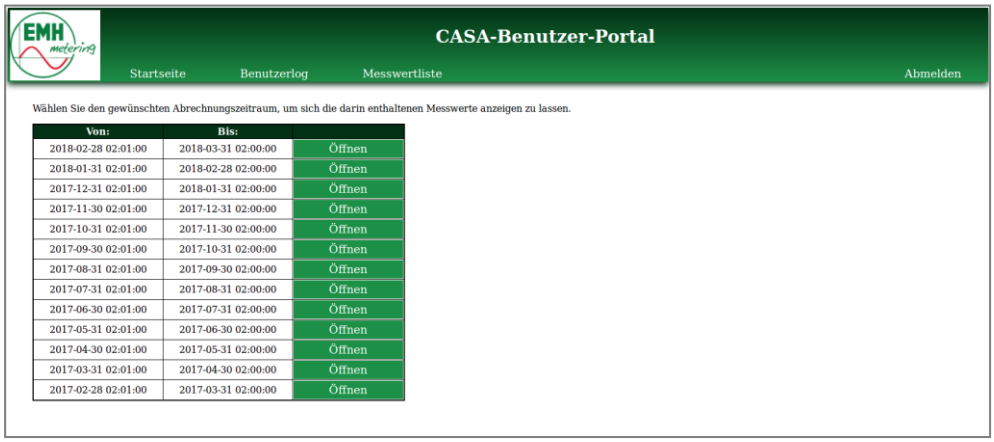


Abbildung 17: Beispielhafte Darstellung der Abrechnungszeiträume eines TAF

2. Es wird eine Liste mit den im TAF-Profil konfigurierten Abrechnungszeiträumen angezeigt.

Bitte beachten Sie, dass die Abrechnungszeiträume, die kürzer als eine Woche sind, solange zusammengefasst werden, bis der angezeigte Zeitraum mindestens eine Woche beträgt.

3. Klicken Sie auf den gesuchten Abrechnungszeitraum.
4. Es wird eine Übersicht der in diesem Zeitraum angefallenen Zählerdaten angezeigt.

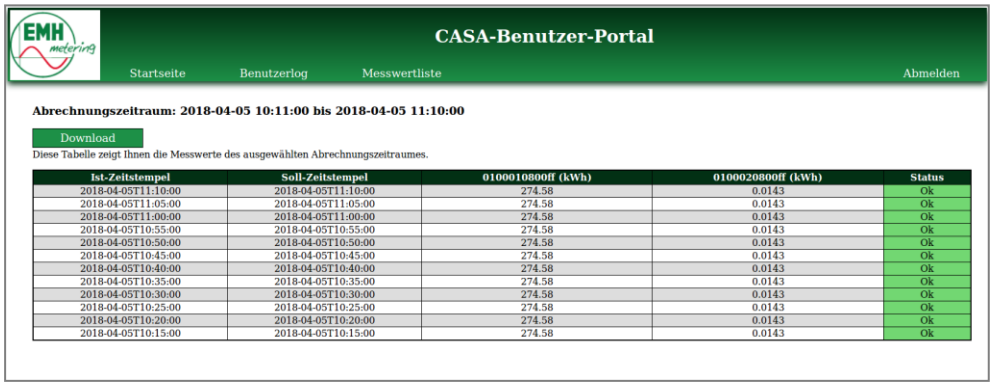


Abbildung 18: Beispielhafte Übersicht der Zählerdaten

Um die Zählerdaten des gewählten Abrechnungszeitraums im CSV-Format herunter zu laden, gehen Sie wie folgt vor:

5. Klicken Sie auf **Download**.
6. Speichern Sie die Datei.

Wie Sie die CSV-Datei in Ihren Texteditor, Ihr Tabellenkalkulationsprogramm oder Ihre Datenbank importieren, entnehmen Sie bitte der jeweiligen Beschreibung der Software.

7.6 Fehlerzustand

Im Falle eines Fehlerzustands (Soft-Lock-Down-Modus, siehe Kapitel 8 „Fehlerbehebung“ / Seite 38) ist keine Anmeldung an der HAN-Schnistelle mehr möglich. Somit können keine personenbezogene Daten (Messwerte, Logbucheinträge) abgerufen werden. Dieser Zustand wird durch folgenden Hinweistext dargestellt:

Abbildung 19: Fehlermeldung im Soft-Lock-Down-Modus

8 Fehlerbehebung

Die Fehlerbehebung erfolgt ausschließlich durch den Gateway-Administrator (GWA) oder auf dessen Anweisung.

Im CASA aufgetretene Fehler werden im Letztverbraucher-Logbuch (siehe Kapitel 7.3 „Letztverbraucher-Logbuch auslesen“ / Seite 34) vermerkt, per Webseite angezeigt (siehe Kapitel 7.6 „Fehlerzustand“ / Seite 37) oder an den LEDs signalisiert (siehe Kapitel 2.3.2 „LEDs an der Frontseite“ / Seite 15).

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-** bzw. in den **Hard-Lock-Down**-Modus.

Im **Soft-Lock-Down**-Modus werden keine Zählerdaten mehr eingesammelt, tarifiert oder versendet und der Letztverbraucher (LV) hat keinen Zugriff mehr. Der Gateway-Administrator (GWA) wird informiert.

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

- Es stehen weniger als 10% Systemspeicher zur Verfügung.
- Der Selbsttest wurde mit einem kritischen Fehler nicht bestanden.
- Das System erkennt eine Hardware-Veränderung.
- Das System verfügt nicht mehr über eine gültige Uhrzeit.

Im **Hard-Lock-Down**-Modus stellt der CASA den Betrieb ein und ist dauerhaft nicht mehr erreichbar, weder für den Gateway-Administrator (GWA), den Service-Techniker (ST) noch für den Letztverbraucher (LV).

Der **Hard-Lock-Down**-Modus wird ausgelöst, wenn

- der CASA im laufenden Betrieb einen Integritätsfehler der Firmware festgestellt hat, den Gateway-Administrator (GWA) formiert hat (soweit möglich), einen Neustart ausgeführt hat und
- der Fehler im Rahmen der Integritätstests während des anschließenden Systemhochlaufs erneut auftritt.

9 Anhang

9.1 Pflegehinweise

Gefahr durch elektrische Spannung

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!

9.2 CASA-Software

Der CASA enthält Software, die unter der General Public Licence (GPL) steht.
Weitere Informationen hierzu können unter http://www.gnu.org/copyleft/gpl.html abgerufen werden.
Der CASA enthält Open Source Komponenten. Nähere Informationen erhalten Sie auf Anfrage.

9.3 Protokollierte Ereignisse im Letztverbraucher-Log

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.

9.3.1 LMN

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

9.3.2 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.

event_id	event_sub_id	Log Level	Text der Meldung
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]

9.3.3 Zeitsynchronistion

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].

9.3.4 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]

9.3.5 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.
4294951295	0	info	Umschaltzeitpunkt für neue Tarifstufe [1] erreicht ([2])

9.3.6 Funktionsüberprüfung

event_id	event_sub_id	Log Level	Text der Meldung
19001	0	fatal	Die Integrität des SMGWs 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	0	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 Eichlogs ist erschöpft. Das Gerät muss ausgetauscht werden.
4294948294	0	warning	Consumerlog für [1] ist voll. Einträge älter als 15 Monate wurden gelöscht
4294948293	0	warning	Es wurden [1] oder mehr ungültige Authentifizierungsversuche registriert ([2]).
4294948286	0	Fatal	Es ist der fatale Fehler [1] im System aufgetreten. 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.
4294948266	0	Info	Das System ist zum ersten Mal oder nach einem unerwarteten Reboot gestartet.

9.3.7 Profilkonfiguration

event_id	event_sub_id	Log Level	Text der Meldung
20003	0	info	Das Kommunikationsprofil [1] wurde aktualisiert. Die Zieladressen sind [2]
20011	0	info	Das Auswerteprofil [1] wurde aktualisiert.
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.

9.4 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 einer der nachfolgend beschrieben Fehler auf, informieren Sie bitte den Messstellenbetreiber (MSB). Dieser beauftragt den Gateway-Administrator (GWA) mit Maßnahmen zur Fehleranalyse und Fehlerbehebung.

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
100064	Interne Prozesskommunikation gestört	
100066	Interne Prozesskommunikation gestört	
100067	Interne Prozesskommunikation gestört	
100070	Interne Prozesskommunikation gestört	
101007	Timer zum Einsammeln und Überprüfen von Zählern gestört	
101008	HDLC-Konfiguration invalide	x
101009	HDLC-Schnittstelle nicht geöffnet	x
101172	Zählerprofil nicht gefunden, ungültiges LMN Zertifikat oder ungültiges Zähler Zertifikat	
101222	Max. Anzahl von Pairingversuche erreicht	
101317	Länge der empfangenen Nachricht zu kurz	
101318	Inkorrekte Nachricht empfangen	
101320	Die Nachricht wurde außerhalb des korrekten Zeitslots empfangen	
101322	Die Nachricht hat einen falschen Frame Format Type oder Port	
101325	Ungültige Antwortzeit, Nachricht wurde zu spät versendet	
101327	Zähler sendet eine "Disconnect Mode" Nachricht. Verbindung wird abgebaut.	
101328	Nachricht mit ungültigen Typ empfangen	
101337	Zähler sendet eine "Disconnect Mode" Nachricht. Verbindung wird abgebaut.	
101338	Unerwartete Nachricht empfangen	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
101519	SYM-MSG-2: Ungültige Paketlänge	
101522	SYM-MSG-2: Nachrichten ohne Versionsangabe nicht unterstützt. Zähler kommt auf Blacklist.	
101535	SYM-MSG-2: Die Nachricht konnte nicht korrekt empfangen werden	
101536	SYM-MSG-3: Die Nachricht konnte nicht korrekt empfangen werden	
101537	SYM-MSG-4: Die Nachricht konnte nicht korrekt empfangen werden	
101538	SYM-MSG-5: Die Nachricht konnte nicht korrekt empfangen werden	
101539	SYM-MSG-1: Die Nachricht konnte nicht korrekt empfangen werden	
101580	SYM-MSG-2: Keine gemeinsame Ciphersuite	
101582	SYM-MSG-2: Keine gemeinsame elliptische Kurve	
102015	Kann keine Kommunikation zum wMBus-Modul aufbauen	
102016	Part-Nummer des wMBus-Moduls ist falsch	x
102017	Unerwartete FW-Version des wMBus-Moduls gefunden	x
102018	wMBus-Konfiguration invalide	x
102019	wMBus-Schnittstelle nicht geöffnet	x
1800200	CLS-Socks-Server nicht gestartet	
1800201	Interne Prozesskommunikation gestört	
1800202	Kein gültiges SMGW HAN-Zertifikat (BP)	
1800117	Verbindung nicht gefunden	
1800118	Fehler beim Laden des CLS-Profiles	
1800119	Verbindung zwischen EMT und CLS ist bereits hergestellt	
1800144	Fehler in der Profilkonfiguration (channel_purpose)	
1800313	Verbindungsaufbau zum CLS-Gerät ist fehlgeschlagen	
1800314	Verbindungsaufbau zum EMT ist fehlgeschlagen	
800802	CON-Server kann keine Anfragen entgegennehmen	
800803	CON-Server kann keine Anfragen entgegennehmen	
800804	CON-Server kann keine Anfragen entgegennehmen	
800805	Interne Prozesskommunikation gestört	
800901	Das installierte Profil ist für HKS1 konfiguriert	
400001	Zugehöriges TAF-Profil nicht gefunden	
400002	Logical_name des OnDemandDelivery-Profils ungültig	
400003	Keine Kommunikationsprofil-Referenz im OnDemandDeliver-Profil gefunden	
400004	Ungültiges meter_reading_date im OnDemandDelivery-Profil	
400005	Kein meter_reading_date im OnDemandDelivery-Profil gefunden	
400012	Interne Prozesskommunikation gestört	
400015	Keine Letztverbraucher-Referenz im zugehörigen TAF-Profil gefunden	
400018	Interne Prozesskommunikation gestört	
400020	Interne Prozesskommunikation gestört	
400204	Interne Prozesskommunikation gestört	
700034	Ein am GWA-Wechsel beteiligter Dienst hat den GWA-Wechsel abgebrochen	
700502	Interne Prozesskommunikation gestört	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
700503	MGMT-Verbindungsstatus inkonsistent	x
500502	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
900696	WAN-A Funkmodul nicht erreichbar	
900697	Funkmodulkonfiguration inkonsistent	x
2200041	Das Zertifikat ist abgelaufen	
2200042	Das Zertifikat hat seinen Gültigkeits-Startzeitpunkt noch nicht erreicht	
2200044	Ein Benutzer mit dem angegebenen Zertifikat existiert nicht	
2300012	Nonce-Generierung mittels Sicherheitsmodul fehlgeschlagen	
2300027	Erstellung der ASN.1 Struktur für komprimierte Daten fehlgeschlagen	
2300028	Erstellung der ASN.1 Struktur AuthAttributes fehlgeschlagen	
2300032	Shared Secret Berechnung durch das Sicherheitsmodul fehlgeschlagen	
2300033	Erstellung der ASN.1 Struktur AuthEnvelopedData fehlgeschlagen	
2300034	Erstellung der ASN.1 Struktur SignedAttributes fehlgeschlagen	
2300035	Erstellung der ASN.1 Struktur SignedData fehlgeschlagen	
2300038	Die MAC-Berechnung ist fehlgeschlagen	
2300045	Nicht ausreichend sicherer Speicher (SRAM) frei	
2300053	Initialisierung (Key-Schedule) der Verschlüsselung oder MAC-Generierung fehlgeschlagen	
2300057	Schlüssel-Generierung mittels Sicherheitsmodul fehlgeschlagen	
2300061	Die symmetrische Verschlüsselungsoperation ist fehlgeschlagen	
2300093	Die Key Wrap Operation ist fehlschlagen	
2300095	Erstellung der Signatur fehlgeschlagen	
2300097	Nicht ausreichend Speicher verfügbar	
2300156	Schlüsselableitung fehlgeschlagen	
2300157	Schlüssel Unwrapping fehlgeschlagen	
2300158	Schlüssellänge passt nicht zum Encryption Mode	
2300159	AES Key Scheduling fehlgeschlagen	
2300160	Entschlüsselung fehlgeschlagen	
2300161	GCM Tag ungültig	
2300162	MAC Berechnung fehlgeschlagen	
2300163	CMAC ungültig	
2300170	Subject Key Identifier passt nicht zum Signaturzertifikat des Gateways	
2300171	Signatur ungültig	
2300172	Struktur des CMS Containers falsch	
2300300	Auslesen des GWA Common Name für neue OU fehlgeschlagen	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
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	
2300315	Laden des Schlüsselobjektes fehlgeschlagen	
1400001	Es wurden doppelte Logfile gefunden, der Fehler wurde behoben	
1400002	Logdatei-Nummerierung inkonsistent	x
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
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
1400560	Fehlerhaftes Dateiattribute gefunden	x
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	x
600028	Fehler beim Erkennen des Profiltyps	x
600029	Fehler beim XML-kodieren des Profils	
600033	Konfigurationssynchronisation gestört	x
600034	Konfiguration setzen gestört	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
600035	Konfiguration lesen gestört	
600036	Konfiguration löschen gestört	
600038	Konfigurationssynchronisation gestört	
600039	Konfigurationssynchronisation gestört	x
600040	Konfigurationssynchronisation gestört	
600041	Konfiguration setzen gestört	
600042	Konfiguration lesen gestört	
600043	Konfiguration löschen gestört	
600044	Konfigurationssynchronisation gestört	
600045	Konfigurationssynchronisation gestört	
600104	Profilvalidierung fehlgeschlagen	
600214	Integritätsprüfung fehlgeschlagen	x
600215	Integritätsprüfung fehlgeschlagen	x
600500	Soft Lock Down Mode aktiv oder interne Prozesskommunikation gestört	
200402	Interne Prozesskommunikation gestört	
200404	Interne Prozesskommunikation gestört	
200405	Die Messwertlisten haben falsche Zugangsrechte	
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	
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	x
1900103	Der Prozess x wurde zu häufig neugestartet	x
1900502	Der Selbsttest läuf bereits und kann nicht erneut ausgeführt werden	
1900503	Das System befindet sich im sLDM, es kann kein selbtest ausgefühgt werden	
1900504	Es wurde ein unerlaubt gestarteter Prozess gefunden	x

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
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	
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 Keys 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 Keys 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	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
1600137	Das Format der AUTH Challenge Response Signatur ist ungültig	
1600138	Interner Fehler im Sicherheitsmodul beim Aktivieren des AUTH Zustandes	
1600140	Interner Fehler im Sicherheitsmodul beim Terminieren des AUTH Zustandes	
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
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	
1200001	Initialisierungsfehler des SRV-Servers	
1200501	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	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
1200506	SRV-Server benutzt falschen Port	x
1200507	Zuviele SRV-Verbindungen zeitgleich offen	x
300018	Interne Prozesskommunikation gestört	
300019	Interne Prozesskommunikation gestört	
2500350	Integritätscheck der Datenbank ist fehlgeschlagen	x
2500351	Integritätscheck der Datenbank kann nicht ausgeführt werden	
2500352	Integritätscheck der Datenbank ist fehlgeschlagen	x
2500353	Integritätscheck der Datenbank kann nicht ausgeführt werden	
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
1500034	Auslesen der RTC fehlgeschlagen	
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
1300116	Fehler der eigentlichen Installation während des Systemstarts	x
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 busabstractor konnte über IPC nicht aufgerufen werden	
2600101	Die Selbsttestfunktion vom busabstractor konnte über IPC nicht aufgerufen werden	

Fehlercode	Beschreibung	Soft-Lock-Down-Modus
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	
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	

9.5 Normen und Richtlinien

Richtlinie 2012/27/EU	Richtlinie des Europäischen Parlaments und des Rates zur Energieeffizienz
IEC 60715	Abmessungen von Niederspannungsschaltanlagen und Geräten Standardisierte Montage auf Schienen zur mechanischen Unterstützung elektrischer Geräte in Schalt- und Geräteanlagen
DIN 43863-5:2012-04	Herstellerübergreifende Identifikationsnummer für Messeinrichtungen
VDE AR-N 4400:2011-09	Anwendungsregel „Messwesen Strom (Metering Code)“
BSI-CC-PP-0073	Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.3 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html
BSI-CC-PP-0077	Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.03 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0077+V2.html
BSI TR-03109-1	Technische Richtlinie „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“
BSI TR-03109-2	CASA – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1
BSI TR-03109-3	Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1
BSI TR-03109-4	Smart Metering PKI - Public Key Infrastruktur für SMGw, Version 1.2.1
BSI TR-03109-6	SMGw Administration, Version 1.0
FNN-Lastenheft Logmeldungen	Lastenheft „Logmeldungen zur Einbindung von SMGw-G1-Geräten“ Version 1.0, 14.06.2016, Forum Netztechnik/Netzbetrieb im VDE (FNN)
CASA-API	CASA 1.0 – SMGw-Schnittstellenbeschreibung (CASA API), Version 1.24
CASA-PHB-ST-GWA-DE	CASA 1.0 – Installations- und Konfigurationshandbuch für Service-Techniker und für Gateway-Administratoren, Version 1.17
CASA-ST	CASA 1.0 – Security Target (CASA-ST), Version 2.00
GPL Lizenz	General Public License

9.6 Abkürzungsverzeichnis

BSI --- Bundesamt für Sicherheit in der Informationstechnik 11
CASA --- Communication Access Security Administrator III
CLS --- Controllable Local System 11
CSV --- Comma-separated values 34
DIN --- Deutsches Institut für Normung e.V. II
EMT --- Externer Marktteilnehmer 29
EnWG --- Energiewirtschaftsgesetz 16
GPL --- General Public Licence 39
GPRS --- General Packet Radio Service 19
GSM --- Global System for Mobile 19
GWA --- Gateway-Administratoren IV
HDLC --- High-Level Data Link Control 15
IEC --- International Electrotechnical Commission 51
LED --- Light emitting Diode/Leuchtdiode 18
LMC --- Local Meter Controller 18
LMN --- Local Meteorological Network 18
MSB --- Messstellenbetreiber IV
OBIS --- Object Identification System 16
PKI --- Public Key Infrastructure 24
PTB --- Physikalisch-technische Bundesanstalt 11
PWR --- Power 18
Root-CA --- Root Certification Authority 24
SHA --- Secure Hash 10
SIM --- Subscriber Identity Module 12
ST --- Service-Techniker IV
TAF - Tarifanwendungsfall 16
TLS --- Transport Layer Security 18
VDE --- Verband Deutscher Elektrotechniker 51
WAN --- Wide Area Network 11
WAN-A --- Wide Area Network-Antenne 18
wMT --- Wireless-MBus-Traffic 18

10 Konformitätserklärung

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

.