

CASA 1.0 und CASA 1.1

Benutzerhandbuch für Letztverbraucher



Die in diesem Handbuch veröffentlichten Inhalte sind urheberrechtlich geschützt.

Übersetzungen, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen bedürfen der ausdrücklichen Genehmigung der EMH metering GmbH & Co. KG.

Alle in diesem Handbuch genannten Warenzeichen und Produktnamen gehören der EMH metering GmbH & Co. KG bzw. den jeweiligen Titelhaltern.

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.

© 2023 EMH metering GmbH & Co. KG. Alle Rechte vorbehalten.

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 54 erläutert sind.

Hinweise zum CASA 1.0 und CASA 1.1 - 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.

Mess- und eichrechtskonforme Verwendung

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

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 Servicetechniker (ST)



Hinweis MSB

Hinweis bzw. Anweisung speziell für den Messtellenbetreiber (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 Servicetechniker (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

Benennung	Handbuch
CASA 1.0 und CASA 1.1 – Installations- und Konfigurationshandbuch für Servicetechniker und für Gateway-Administratoren	[CASA-PHB-ST-GWA-DE]
CASA 1.0 und CASA 1.1 – Benutzerhandbuch für Letztverbraucher	[CASA-PHB-LV-DE]
CASA 1.0 und CASA 1.1 – SMGw-Schnittstellenbeschreibung (CASA API)	[CASA-API]
CASA – Betriebshinweise für eine mess- und eichrechtkonforme Verwendung	[CASA-PHB-MessEG-DE]

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	Beschreibung
Rev. 1.17	14.12.2019	Dokumentationsstand der Erstzertifizierung
Rev. 1.18	20.03.2020	S. VI: Dokumentenhistorie um Arbeits- und Zwischenstände bereinigt Kap. 2.2: Abbildung 1 und Software-Versionsnummer aktualisiert Kap. 2.3.1: Abbildung 4 aktualisiert Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.24	24.02.2021	Einleitung: Hinweis zur mess- und eichrechtskonformen Verwendung ergänzt Kap. 2.2: Abbildung 1 und Software-Versionsnummer aktualisiert Kap. 2.4.2: Beschreibung zu TAF9 und TAF14 hinzugefügt, Beschreibung zu TAF 10 erweitert Kap. 7.2: Abbildung 11 aktualisiert Kap. 7.7: Abschnitt zum Nachvollziehen der Tarifierung und Abrechnung hinzugefügt Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.25	08.06.2021	Kap. 2.2: Abbildung 1 und Software-Versionsnummer aktualisiert Kap. 2.6, Tabelle 4: Normenangabe der Safety-Prüfung aktualisiert, WAN-A mit GPRS entfernt Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.50	14.07.2022	Kap. 2.2: Abbildung 1 und Software-Versionsnummer aktualisiert und CASA 1.1 ergänzt Kap. 2.6: Technische Daten aktualisiert. Kap. 2.4.1, TAF 14: Hinweis zur kleinstmöglichen Abtastperiode entfernt. Kap. 6.2: Hinweis zu Konfigurationsmöglichkeiten des Servicetechnikers ergänzt. Kap. 7.2ff: Abbildungen zur Web-Oberfläche an der HAN-Schnittstelle aktualisiert. Kap. 7.2: Hinweise zur Verwendung von Host-Namen zur Adressierung der HAN-Schnittstelle und zur Handhabung von selbstsignierten TLS-Zertifikaten ergänzt. Kap. 9.3: Logmeldungen aktualisiert. Kap. 9.5: Dokumentenreferenzen aktualisiert
Rev. 1.51	09.03.2023	Kap. 1.3: CC-Verfahrensnummer aktualisiert. Kap. 2.2.2 zur Beschriftung des CASA 1.1 hinzugefügt. Kap. 2.3: Abbildung 3 aktualisiert. Kap. 2.3.1, Abbildung 4 und Titelseite: Foto aktualisiert. Kap. 2.3.2: Tabelle 2: Weitere Anzeigefunktionen der LMC-LED ergänzt. Kap. 2.4.2: Abtastperiode für TAF 14 ergänzt. Kap. 2.6, Tabelle 4: Technische Daten aktualisiert. Kap. 7.5: Beschreibung zur Anzeige der JSON-Daten hinzugefügt. Kap. 9.3: Logmeldungen aktualisiert. Kap. 9.4: Fehlercodes aktualisiert.
Rev. 1.52	16.03.2023	Kap. 2.6, Tabelle 4: Hinweis zu Informationen zum Installationsstatus angepasst. Kap. 9.5: Dokumentenreferenzen aktualisiert. Kap. 9.6: Abkürzungen ergänzt.
Rev. 1.53	15.06.2023	Kap. 2.2.1: Abbildung 1 und Software-Versionsnummer aktualisiert
Rev. 1.54	31.07.2023	Kap. 2.2.1: Abbildung 1 und Software-Versionsnummer aktualisiert
Rev. 1.55	14.08.2023	Kap. 9.5: Dokumentenreferenzen aktualisiert.

Inhaltsverzeichnis

Einleitung	III
Hinweise zum CASA 1.0 und CASA 1.1 - Benutzerhandbuch für Letztverbraucher	III
Zielgruppe	III
Geltungsbereich	III
Bestimmungsgemäßer Gebrauch	III
Mess- und eichrechtskonforme Verwendung	III
Wartungs- und Gewährleistungshinweise	III
Verwendete Symbole und Warnhinweise	IV
Dokumentationskonzept	V
Dokumentation zu diesem Produkt	V
Historie VI	
Inhaltsverzeichnis	VII
1 Allgemeine Sicherheitshinweise	9
1.1 Sicherheitshinweise	9
1.2 Maßnahmen und Sicherheitsziele	9
1.3 Integritätssicherung der Dokumentation	9
2 Gerätebeschreibung	11
2.1 Kurzbeschreibung	11
2.2 Beschriftung des Gerätes	12
2.2.1 Beschriftung des CASA 1.0	12
2.2.2 Beschriftung des CASA 1.1	13
2.3 Gehäuse- und Anzeigeelemente	14
2.3.1 CASA mit HAN-Modul	15
2.3.2 LEDs an der Frontseite	16
2.3.3 LEDs an den Schnittstellen	16
2.4 Funktionen des CASA	17
2.4.1 Messwerte für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung	17
2.4.2 Anwendungsfälle	17
2.5 Firmware-Update	19
2.6 Technische Daten – CASA 1.0 und CASA 1.1	20
3 Sicherheit	22
3.1 Prüfung der Integrität des CASA	22
3.2 CASA Sicherheitssiegel	22
3.2.1 Position des Sicherheitssiegels	22
3.2.2 EMH Sicherheitssiegel	23
3.2.3 Unbeschädigte Sicherheitssiegel	24
3.2.4 Beschädigte Sicherheitssiegel	24
4 Kommunikation	26
4.1 Externe Kommunikationswege des CASA	26
4.2 Interne Kommunikation und Sicherheitskonzept des CASA	26
4.2.1 Softwaresicherheitskonzept	26
4.2.2 Schutz der gespeicherten Messwerte gegen Verfälschung	26
4.2.3 Schutz des Programmcodes	26
4.2.4 Schutz von übertragenen und gespeicherten Daten	27
4.2.5 Fehlererkennung der Zählerdaten	27
4.3 Kommunikationsprotokolle	27
4.4 Inhaltsdatensicherung und Signaturbildung	27
4.5 Pseudonymisierung von Daten	27

5	Logbücher	29
5.1	Logbücher allgemein.....	29
5.2	Letztverbraucher-Log.....	29
5.3	System-Log.....	30
5.4	Eich-Log.....	30
6	Rollen und Zugriffsberechtigungen	31
6.1	Gateway-Administrator (GWA)	31
6.2	Servicetechniker (ST).....	31
6.3	Letztverbraucher (LV)	31
6.4	Externe Marktteilnehmer (EMT).....	31
6.5	Messstellenbetreiber (MSB).....	32
6.6	Identifizierung und Authentifizierung.....	32
7	Der Letztverbraucher (LV)	33
7.1	Rolle des Letztverbraucher (LV)	33
7.2	Kommunikationsverbindung einrichten.....	33
7.3	Letztverbraucher-Logbuch auslesen	36
7.4	Selbsttest auslösen.....	37
7.5	Messwertlisten auslesen.....	38
7.6	Fehlerzustand	39
7.7	Nachvollziehen der Tarifierung und Abrechnung	40
8	Fehlerbehebung	41
9	Anhang	42
9.1	Pflegehinweise	42
9.2	CASA-Software.....	42
9.3	Protokollierte Ereignisse im Letztverbraucher-Log.....	42
9.3.1	LMN.....	42
9.3.2	HAN-Schnittstelle + CLS-Gerät.....	42
9.3.3	Operative Betriebsbereitschaft.....	43
9.3.4	Zeitsynchronisation	43
9.3.5	Selbsttest.....	44
9.3.6	Messwertübertragung	44
9.3.7	Funktionsüberprüfung	44
9.3.8	Profilkonfiguration.....	45
9.3.9	Messwertverarbeitung.....	45
9.4	Herstellerspezifische Fehlercodes.....	46
9.5	Normen und Richtlinien.....	53
9.6	Abkürzungsverzeichnis	54
10	Konformitätserklärung	55

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 20).
- 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 Servicetechniker (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 and CASA 1.1 Security Target (CASA-ST)“ (siehe [CASA-ST]) geführt, das Bestandteil des Common-Criteria-Zertifizierungsverfahrens mit der ID BSI-DSC-CC-0919V3 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 Energieversorgungsunternehmen werden die Messwerte gesammelt, signiert und gespeichert, um anschließend über eine Wide Area Network-Schnittstelle (WAN) an berechnete 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. Servicetechniker (ST) Systeminformationen abrufen.

2.2 Beschriftung des Gerätes

2.2.1 Beschriftung des CASA 1.0

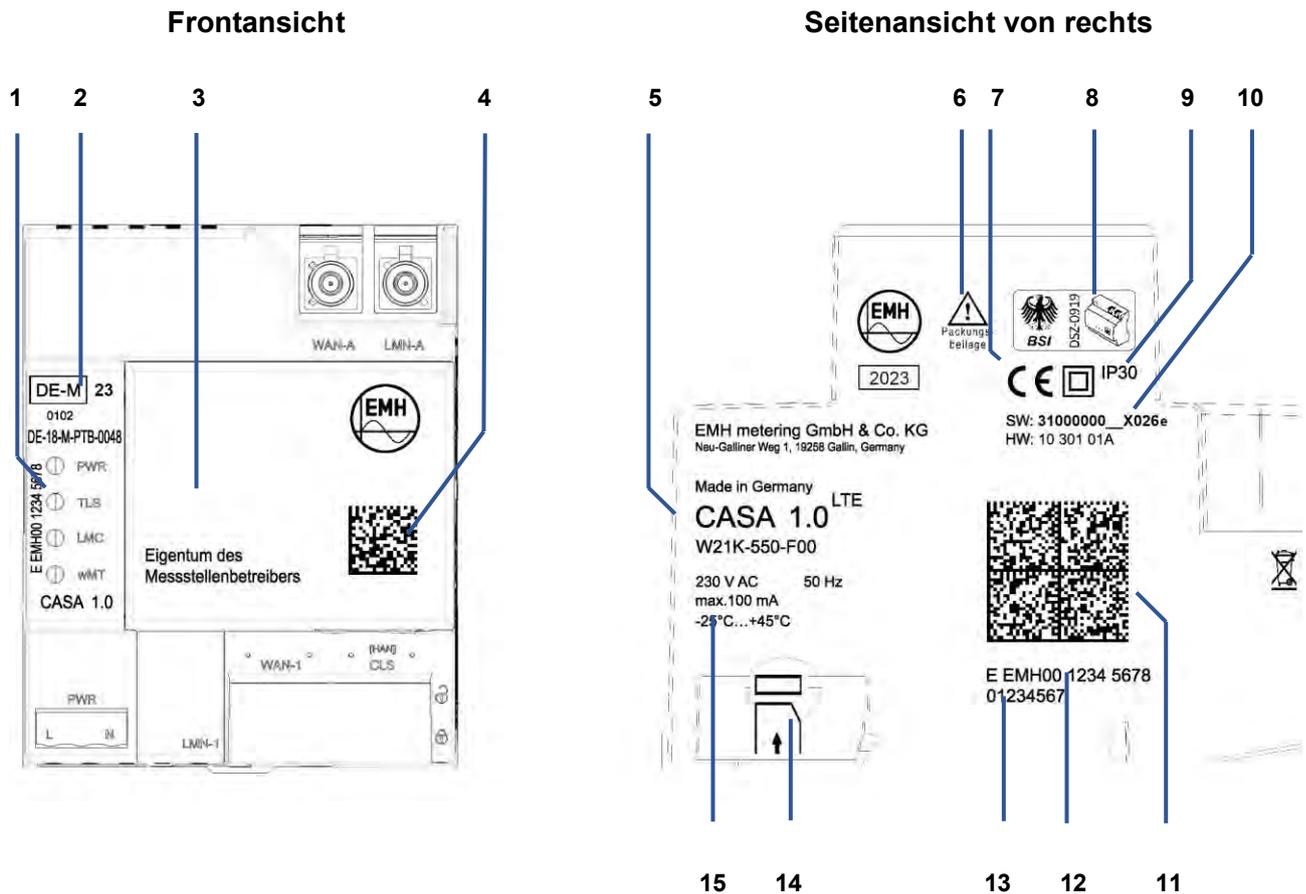


Abbildung 1: CASA 1.0 – Frontansicht und Seitenansicht von rechts

1	Herstellerübergreifende Identifikationsnummer (HÜID)
2	Konformitätskennzeichnung und Nummer der Baumusterprüfbescheinigung der PTB
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
9	Schutzart und Schutzklasse
10	SW: Software-Version (zum Zeitpunkt der Herstellung): 31000000_X026e HW: Hardware-Version (siehe auch Erläuterung im Kap. 2.2.2 unten) 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

2.2.2 Beschriftung des CASA 1.1

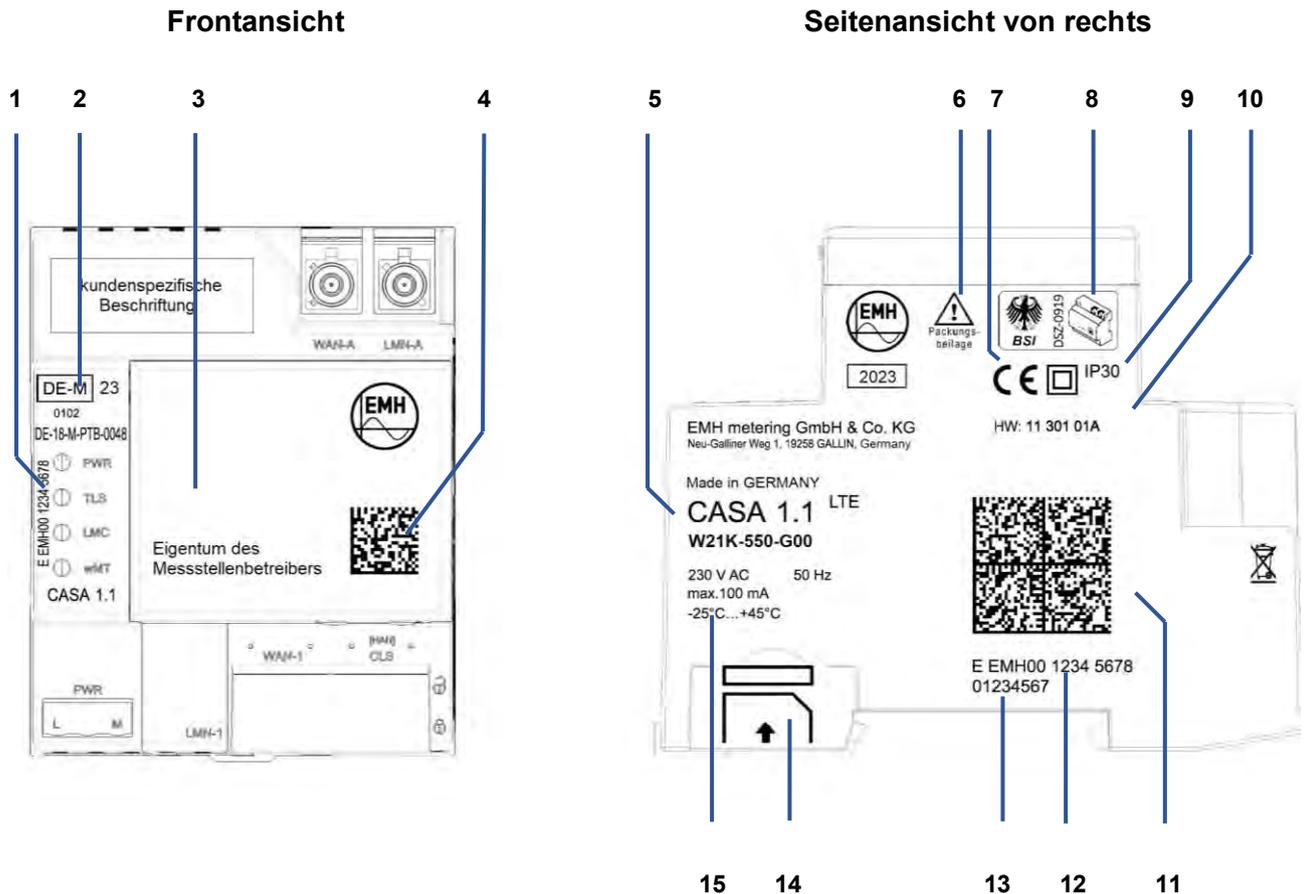


Abbildung 2: CASA 1.1 – Frontansicht und Seitenansicht von rechts

1	Herstellerübergreifende Identifikationsnummer (HÜID)
2	Konformitätskennzeichnung und Nummer der Baumusterprüfbescheinigung der PTB
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
9	Schutzart und Schutzklasse
10	HW: Hardware-Version (siehe auch Erläuterung im Kasten unten) mögliche Hardware-Versionen bei Verwendung von funktionsgleichen Alternativbauteilen: 11 301 xxx 11 302 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



Die in der Gehäusebeschriftung enthaltene Hardware-Version beschreibt in den ersten fünf Stellen den Hardware-Stand des zertifizierungsrelevanten Teils des CASA: Ziffern „10 301“ in Abbildung 1 und „11 301“ in Abbildung 2. 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 und „01A“ in Abbildung 2.

2.3 Gehäuse- und Anzeigeelemente

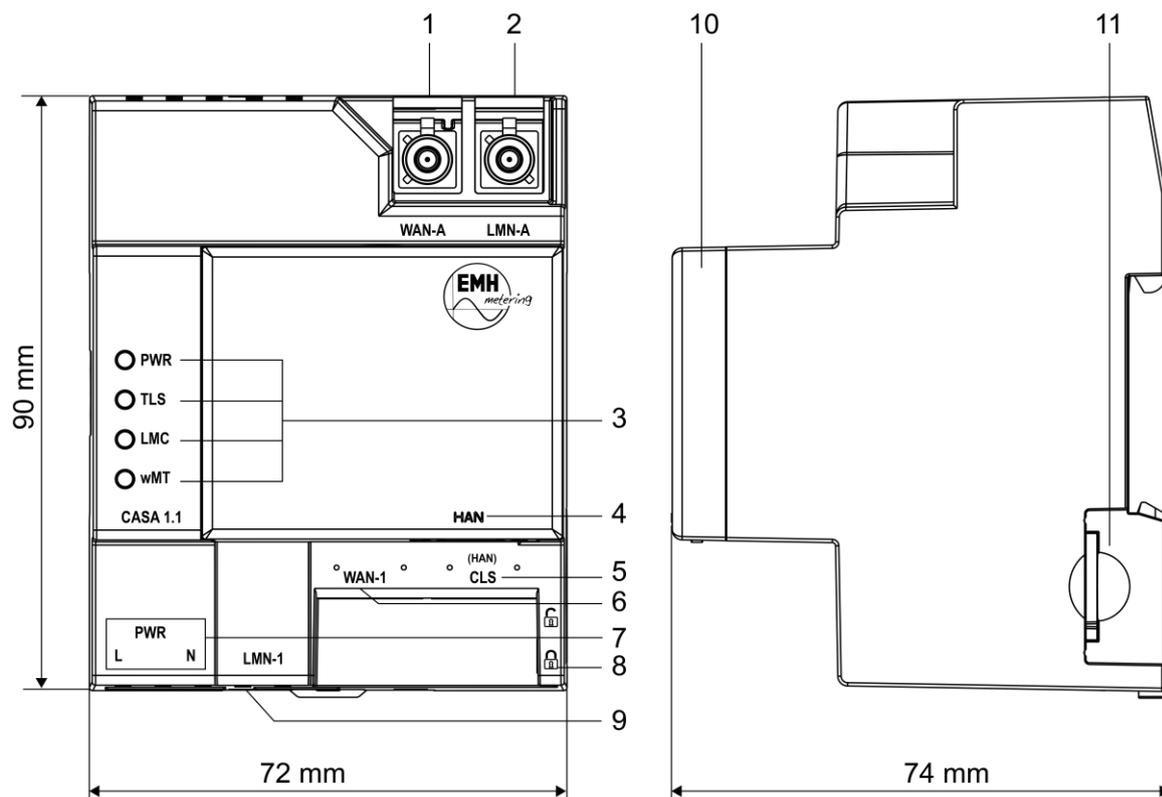


Abbildung 3: Frontansicht (links) Seitenansicht von rechts (rechts)

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 16)
4	HAN-Schnittstelle RJ45
5	[HAN] CLS-Schnittstelle RJ45
6	WAN-1-Schnittstelle RJ45
7	Anschluss für Betriebsspannung 230 V (PWR)
8	Verriegelung für Mehrwertmodul
9	LMN-1-Schnittstelle RJ12-RS485
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 4 / Seite 15 dargestellt.



Abbildung 4: 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	<p>Aus solange die Initialisierung der Firmware läuft.</p> <p>Blinkt bei Abschluss der Initialisierung. Die Dienste der Firmware werden nun gestartet.</p> <p>Leuchtet dauerhaft, wenn die physische Betriebsbereitschaft hergestellt ist, d.h. alle Dienste der Firmware gestartet und betriebsbereit sind.</p> <p>Heartbeat (zweimal schnell blinken, lange Pause), wenn sich das Gerät im Soft Lock-Down Mode befindet und durch einen Gateway-Administrator (GWA) kontrolliert werden muss (siehe auch dazu Kapitel 8 „Fehlerbehebung“ / Seite 41).</p>
TLS (grün)	Transport Layer Security	<p>Blinkt ab Beginn des Aufbaus des TLS-Kanals.</p> <p>Leuchtet dauerhaft, wenn die TLS-Verbindung zum Gateway-Administrator (GWA) mittels eines Wirkzertifikats erfolgt ist (Normalbetrieb).</p> <p>Blinkt, wenn die TLS-Verbindung zum Gateway-Administrator (GWA) mittels eines Gütesiegelzertifikats erfolgt ist.</p> <p>Aus, wenn die Verbindung zum Gateway-Administrator (GWA) getrennt wurde.</p>
LMC (grün)	Local Meter Controller	<p>Leuchtet dauerhaft, wenn für mindestens einen Zähler im Local Metrological Network (LMN) eine High-Level Data Link Control (HDLC)-Adresse vergeben wurde.</p> <p>Aus, wenn keine HDLC-Adresse im LMN vergeben wurde.</p> <p>Wenn der CASA entsprechend konfiguriert ist, können zusätzlich folgende Informationen angezeigt werden:</p> <p>Heartbeat (zweimal schnell blinken, lange Pause), wenn eine Überlastsituation der Stromversorgung für den LMN-Bus erkannt wurde.</p> <p>Blinkt (0,5 Sekunden), wenn die Systemzeit ungültig ist (wird nur angezeigt, wenn gleichzeitig mindestens eine HDLC-Adresse am LMN vergeben ist.)</p>
wMT (blau)	Wireless M-Bus Traffic	<p>Leuchtet kurz auf, wenn ein Wireless-M-Bus-Datensatz empfangen wird.</p>
PWR, TLS, LMC, wMT	Hard Lock-Down Mode	<p>Es blinken alle 4 LEDs dauerhaft, wenn sich das Gerät im Hard Lock-Down Mode (siehe auch dazu Kapitel 8 „Fehlerbehebung“ / Seite 41) befindet und getauscht werden muss.</p>

Tabelle 2: LEDs am CASA

2.3.3 LEDs an den Schnittstellen

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

Tabelle 3: LEDs an den Schnittstellen



Die LEDs an den Schnittstellen dienen ausschließlich zur Erkennung der korrekten Installation durch den Servicetechniker (ST) 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 abrechnungsrelevanten 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.

TAF9 – Bereitstellung der Ist-Einspeisung einer Erzeugungsanlage

Dieser Anwendungsfall erlaubt die Bereitstellung der Ist-Einspeiseleistung an Anlagen nach dem Erneuerbare-Energien-Gesetz und dem Kraft-Wärme-Kopplungsgesetz. Der CASA unterstützt in diesem Zusammenhang die folgenden Ereignisse zum Auslösen des Datenversands:

- Versand im Bedarfsfall (Veranlassung durch den Gateway-Administrator, GWA)
- periodischer Versand
- Versand bei Schwellwertüber- oder unterschreitung

Als Eingangsgrößen für den TAF9 können die Momentanwerte der Gesamt-Einspeisewirkleistung (P_{ges}) und die Momentanwerte der Einspeisewirkleistung einzelner Phasen ($P_{L(1-3)}$) konfiguriert werden.

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



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.

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:

- Versand im Bedarfsfall (Veranlassung durch den Gateway-Administrator, GWA)
- periodischer Versand
- Versand bei Schwellwertüber- oder unterschreitung

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

- Momentanwert der Gesamtwirkleistung P_{ges} ,
- Momentanwert der Phasenwirkleistung $P_{L(1-3)}$
- 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 $I_{L(1-3)}$
- Phasenspannung $U_{L(1-3)}$

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



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.



TAF14 – Hochfrequente Messwertbereitstellung für Mehrwertdienste

Dieser Anwendungsfall erlaubt die hochfrequente Auslesung und Bereitstellung von Messwerten. In der aktuellen Version des CASA beträgt die kleinste Abtastperiode 60 Sekunden. Der CASA unterstützt für diesen Anwendungsfall die folgenden Ereignisse zum Auslösen des Datenversands:

- periodischer Versand,
- Ad-hoc-Versand (jeder eingehender Messwert wird direkt versandt)
- Versand bei Schwellwertüber- oder unterschreitung

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

Für den TAF14 stehen folgende Eingangsgrößen zur Verfügung:

- Gesamtwirkarbeit in Richtung A+
- Phasenwirkarbeit in Richtung A+ für $L_{(1-3)}$
- Gesamtwirkarbeit in Richtung A-
- Phasenwirkarbeit in Richtung A- für $L_{(1-3)}$
- Blindarbeit in Richtung $R_{(1-4)}$
- Momentanwert der Gesamtwirkleistung P_{ges}
- Momentanwert der Phasenwirkleistung $P_{L(1-3)}$



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.



Die Tarifierungsanwendungsfälle TAF3 ... TAF5, TAF8 und TAF11 ... TAF13 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 – CASA 1.0 und 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: Informationen zum Installationsstatus
Geräteschnittstellen (nach Geräteausführung)	Zählerschnittstellen Kundenschnittstellen Weitbereichsschnittstellen	LMN-1, LMN-A HAN, [HAN] CLS WAN-1, WAN-A
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 DIN EN 50470-1
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 transparent: Polycarbonat, halogenfrei, recycelbar nicht transparent: Polycarbonat glasfaserverstärkt, halogenfrei, recycelbar gemäß IEC 62052-31, Kunststoffe gemäß UL94V-0
Umgebungsbedingungen	mechanisch elektromagnetisch vorgesehener Einsatzort	M1 gemäß Messgeräte-Richtlinie (2014/32/EU) E2 gemäß Messgeräte-Richtlinie (2014/32/EU) Innenraum gemäß EN 50470-1
Gewicht		ca. 200 g
LMN-1 RS485	Ausgangsspannung Strombelastbarkeit 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	Mode T/C (gemäß EN 13757-4 inkl. OMS TR 07 Kompaktprofil und nach [BSI-TR-03109-1-Detail- spezifikation]) FAKRA-Stecker, C-codiert, blau

HAN Ethernet	Ethernet	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i)
	Anschluss	8P8C-Buchse (RJ45)
[HAN] CLS Ethernet	Ethernet	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i)
	Anschluss	8P8C-Buchse (RJ45)
WAN-A LTE (Fallback GPRS)	Frequenzbereiche	LTE-Modul (Fallback EDGE/GPRS), Triband (Band 3 / 1800 MHz; Band 8 / 900 MHz; Band 20 / 800 MHz)
	Anschluss	FAKRA-Stecker, D-codiert, bordeaux-violett
WAN-A (optional) LTE-450	Frequenzbereiche	LTE-Modul (Band 31, Band 72 / 450 MHz)
	Anschluss	FAKRA-Stecker, D-codiert, bordeaux-violett
WAN-1 Ethernet	Ethernet	100Base-TX IEEE 802.3 Clause 25 (IEEE 802.3 u) 10Base-T IEEE 802.3 Clause 14 (IEEE 802.3 i)
	Anschluss	8P8C-Buchse (RJ45)

Tabelle 4: Technische Daten

Technische Änderungen vorbehalten!

3 Sicherheit

3.1 Prüfung der Integrität des CASA



Die Integrität des CASA muss vor der Montage und Inbetriebnahme durch den Servicetechniker (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 22.



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.

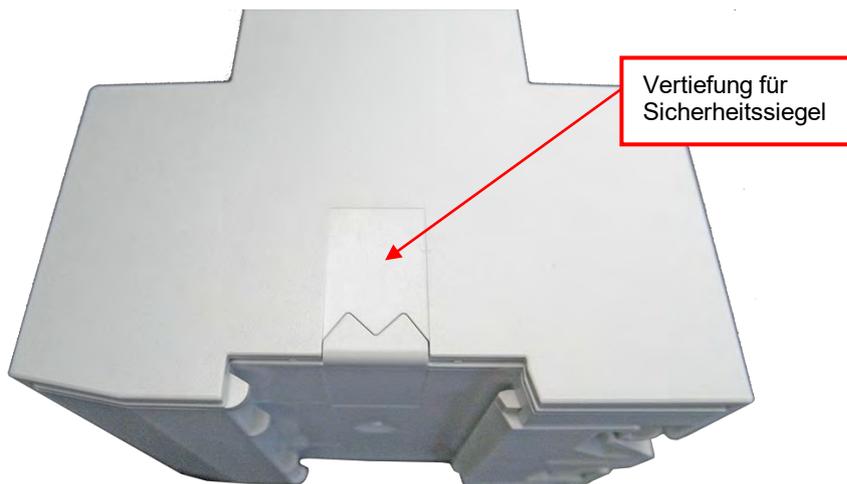


Abbildung 5: Vertiefung für die Position des Sicherheitssiegels

3.2.2 EMH Sicherheitssiegel

Die Gesamtansicht des Siegels bei Beleuchtung mit Tageslicht und seine Abmessungen zeigt Abbildung 6.

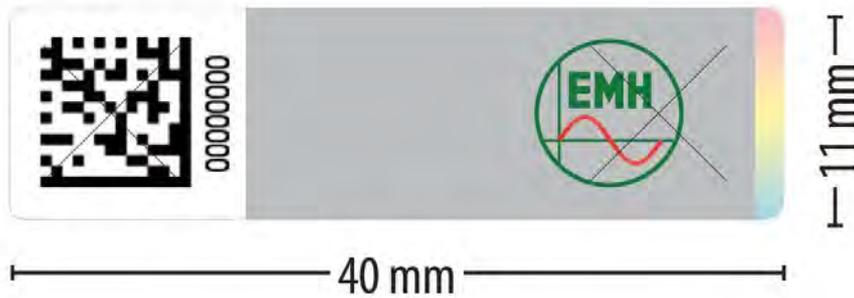


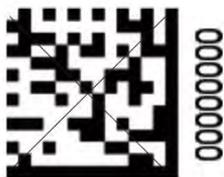
Abbildung 6: Gesamtansicht des Sicherheitssiegels

Bei Beleuchtung mit UV-Licht wird das gelb-grünlich leuchtende Sicherheitsmerkmal des Siegels wie in Abbildung 7 dargestellt erkennbar.



Abbildung 7: Ansicht des Sicherheitssiegels unter UV-Licht

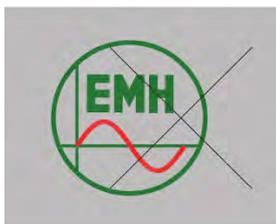
Weitere Sicherheitsmerkmale des Sicherheitssiegels im Detail zeigt die nachfolgende Abbildung 8.



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 8: Sicherheitsmerkmale des Sicherheitssiegels

3.2.3 Unbeschädigte Sicherheitssiegel



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

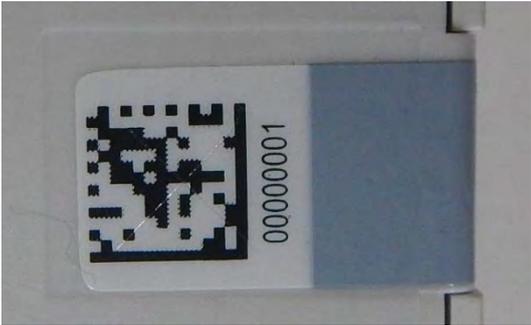
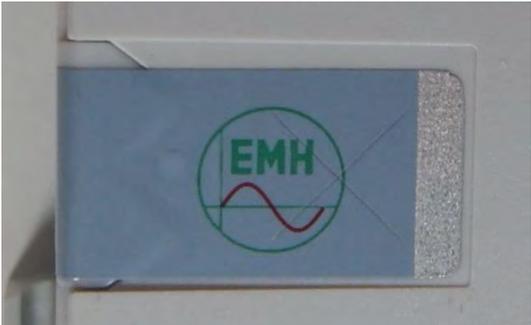
Unbeschädigte Siegel	Beschreibung
	<p>korrektes Siegel</p> 
	<p>korrektes Siegel</p> 
	<p>korrektes Siegel</p> 

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

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

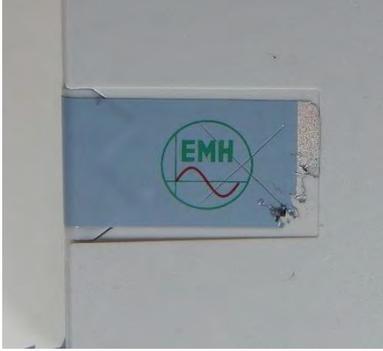
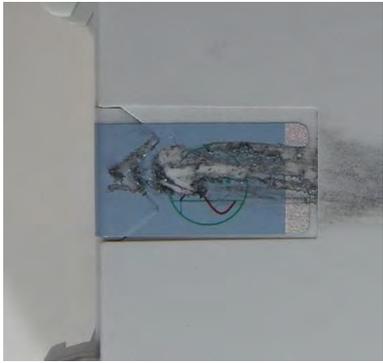
Beschädigte Sicherheitssiegel	Beschreibung
	<p>zerstörtes Sicherheitssiegel nach mechanischem Manipulationsversuch</p> <p style="text-align: center;">X</p>
	<p>zerstörtes Sicherheitssiegel nach mechanischem Manipulationsversuch</p> <p style="text-align: center;">X</p>
	<p>zerstörtes Sicherheitssiegel nach Manipulationsversuch mit chemischen Lösemitteln</p> <p style="text-align: center;">X</p>
	<p>zerstörtes Sicherheitssiegel nach mechanischem Manipulationsversuch mit Kälteeinwirkung</p> <p style="text-align: center;">X</p>
	<p>zerstörtes Sicherheitssiegel nach Manipulationsversuch mit Wärmeeinwirkung</p> <p style="text-align: center;">X</p>

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 angebotenen 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 Softwaresicherheitskonzept

- 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), Servicetechniker (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 31.
- Abrechnungsrelevante 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 (nur bei abrechnungsrelevanten Daten). 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. 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 Messwerte, die im Rahmen eines TAF9 oder TAF10 erfasst werden, können vor der Übertragung an den externen Marktteilnehmer (EMT) oder den Gateway-Administrator (GWA) pseudonymisiert werden. 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 Servicetechniker (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 42.

5.3 System-Log

- Der Zweck des Systems-Logs ist es, den Gateway-Administrator (GWA) und den autorisierten Servicetechniker (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 Servicetechniker (ST)



Der Servicetechniker (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 30) und grundlegende Systemeinstellungen vorzunehmen (siehe [CASA-API]-Dokument Kap. 7.3).

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 Messstellenbetreiber (MSB) ist für die Messstelle und auch für deren Einrichtung verantwortlich. Er nimmt den vom Hersteller gelieferten CASA entgegen und beauftragt einen Servicetechniker (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 Messstellenbetreibers 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 Servicetechnikers (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 „Softwaresicherheitskonzept“ / Seite 26). 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 36)



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 Letztverbraucher (LV) erforderlichen Parameter auf der Ebene des HTTPS-Protokolls sind im Detail im [CASA-API]-Dokument im Kapitel 7 beschrieben (siehe auch Kapitel 9.5 „Normen und Richtlinien“ / Seite 53).

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 7.4 beschrieben.

7.2 Kommunikationsverbindung einrichten



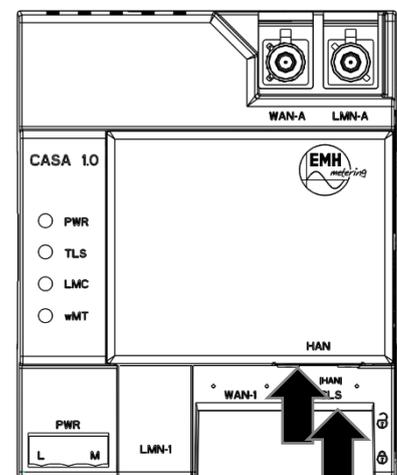
Um Ihre Zählerdaten einzusehen, gehen Sie wie folgt vor:

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 Netzwerkanschlussbuchse Ihres Laptops oder PCs.





Das Auslesegerät und das benötigte Netzkabel 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.

- 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

Anstelle der IP-Adresse können auch die Bezeichner **smgw.local** oder **<HUID>.local** verwendet werden, wobei **<HUID>** der herstellerübergreifenden ID des CASA entspricht, also bspw.:

https://eemh0009264154.local

Da der CASA ein selbstsigniertes TLS-Zertifikat auf der HAN-Schnittstelle verwendet, erscheint ggf. eine Sicherheitswarnung Ihres Browsers. Um auf das Gerät zugreifen zu können, müssen Sie es als Ausnahme hinzufügen:

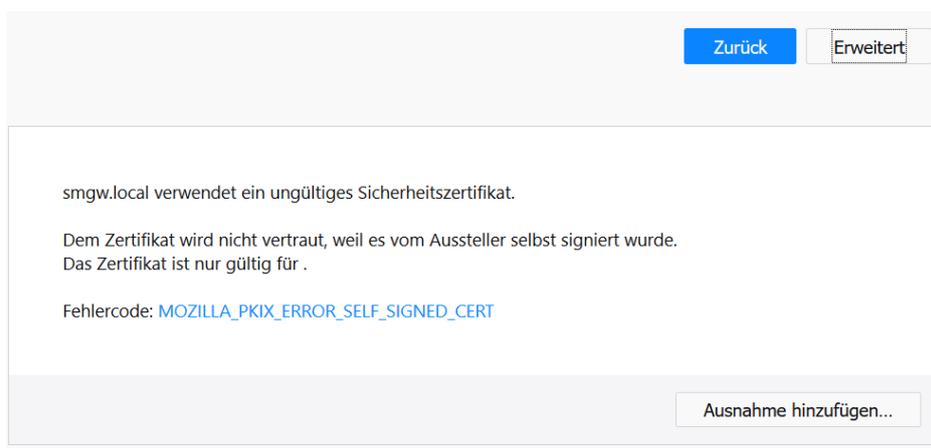


Abbildung 9 - Sicherheitswarnung im Firefox-Browser

- Wählen Sie anschließend die Authentifizierungsmethode:

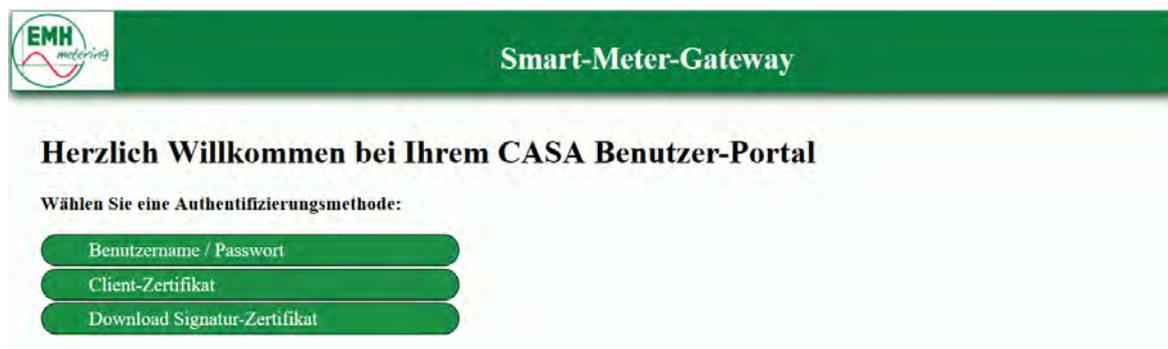


Abbildung 10: Beispiel für das CASA Benutzer-Portal

- Authentifizieren Sie sich entweder mit der vom Gateway-Administrator (GWA) übermittelten Benutzername-Passwort-Kombination oder Ihrem TLS-Client-Zertifikat.
 - Es öffnet sich die Startseite des **CASA-Benutzer-Portals**.

Alternativ können Sie durch Auswahl der Schaltfläche „Download Signatur-Zertifikat“ das Signaturzertifikat des CASA¹ herunterladen, das zur Signaturprüfung der Messwerte benötigt wird.



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 (LV) bezieht sich auf den gesamten Letztverbraucherzugang.



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

Startseite

Hier werden Ihnen aktuelle Systeminformationen des Smart-Meter-Gateways angezeigt:

Systeminformationen			
Systemzeit (CASA): 2022-06-27 15:07:52 ✓	Firmware Version: 290000000X026a	HüID: eemh0009264154	Benutzer-ID: hks2

Diese Tabelle zeigt die Zählerstände aller Ihnen zugeordneten Zählwerke. Über den Link neben der Zählerbezeichnung gelangen Sie zu der JSON-Repräsentation der Messwertdaten.

Aktuelle Zählerstände		
0a01454d480000000001 JSON		
Zeitstempel	Register	aktueller Wert
2022-06-27 15:07:52	0100010800ff	23.163,627000 kWh
2022-06-27 15:07:52	0100020800ff	22.491,413000 kWh
0a01454d480000000002 JSON		
Zeitstempel	Register	aktueller Wert
2022-06-27 15:07:52	0100010800ff	20.868,494000 kWh
2022-06-27 15:07:52	0100020800ff	19.516,854000 kWh

Über den Download-Button können Sie sich das Signatur-Zertifikat zum Überprüfen der Zählerwerte aus der Messwertliste herunterladen.

Signatur-Zertifikat

Über den Auslösen-Button können Sie einen Selbsttest alle 24 Std. ausführen, um den Zustand des Smart-Meter-Gateways zu überprüfen.

Selbsttest-Auslösen

Abbildung 11: 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 CASA¹.
- 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 7.4.2.2 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.

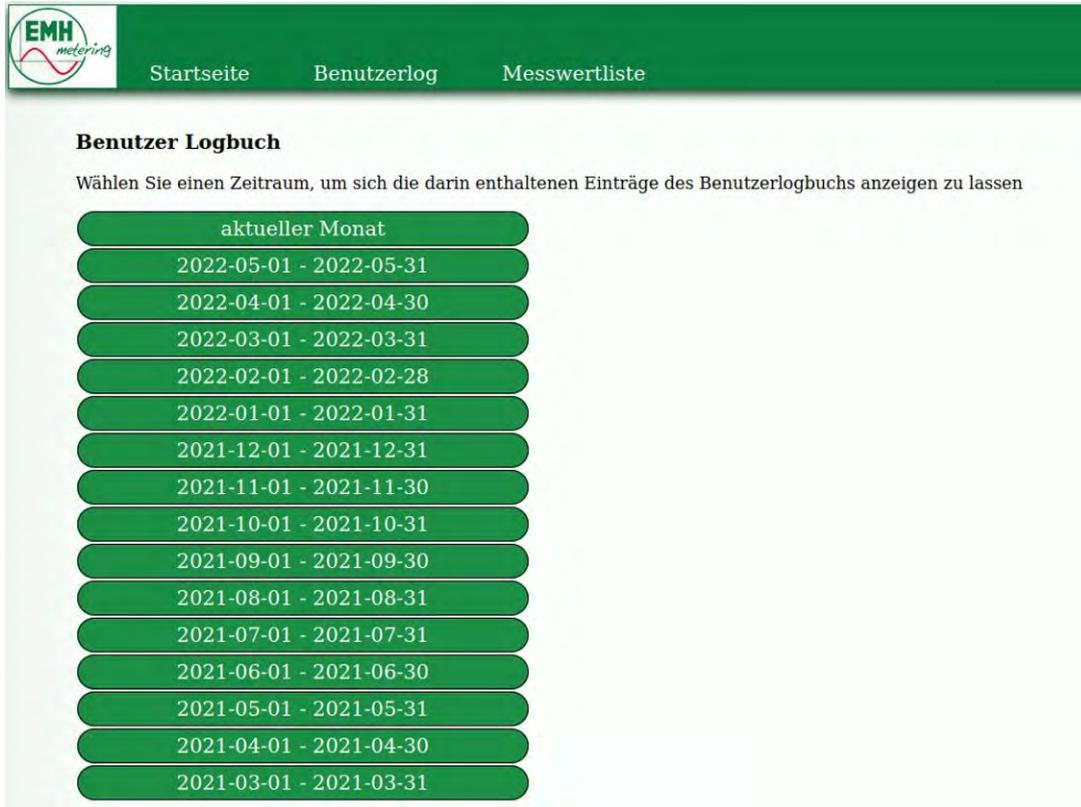


Abbildung 12: Beispiel für ein Benutzer Logbuch

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

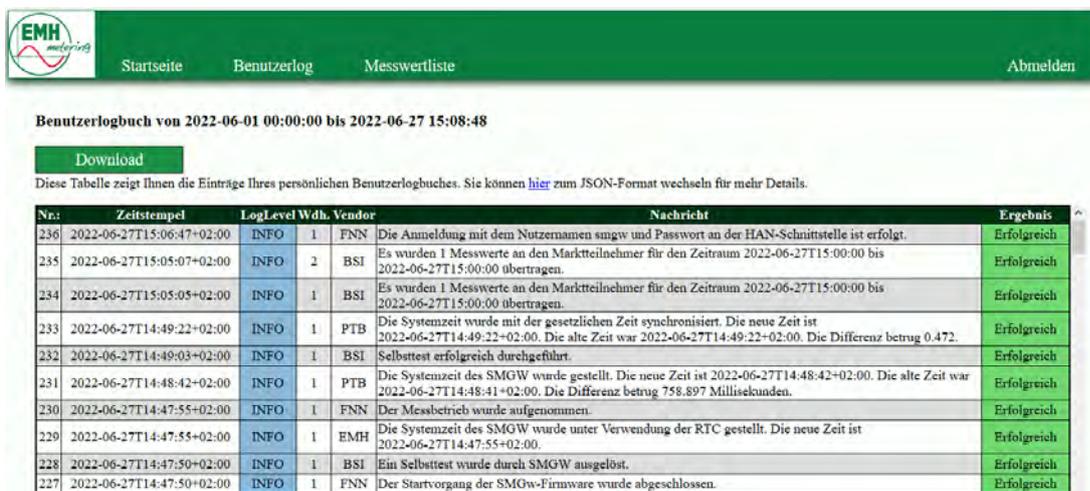


Abbildung 13: Beispielhafte Darstellung für Letztverbraucher-Log



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

Zeitraum	Abgleich
2019-06-26 14:59:53	0100010800ff
2019-06-26 14:59:53	0100020800ff

Über den Download-Button können Sie sich das Signatur-Zertifikat zum Überprüfen der Zählerwerte aus der Messwertliste herunterladen:

Signatur-Zertifikat

[Download](#)

Über den Auslösen-Button können Sie einen Selbsttest alle 24 Std. ausführen, um den Zustand des Smart-Meter-Gateways zu überprüfen.

Selbsttest-Auslösen

[Auslösen](#)

Abbildung 14: Ausführung eines Selbsttests

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

Selbsttest

Der Selbsttest wurde ausgelöst. Es kann einige Minuten dauern, bis das Ergebnis vorliegt. Sie finden das Ergebnis in Ihrem Benutzerlogbuch.

[Zurück](#)

Abbildung 15: Anzeige nach Start des Selbsttests

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

Selbsttest

Es kann nur ein Selbsttest alle 24 Stunden ausgelöst werden. Der nächste Selbsttest ist am **2019-11-22** um **15:31:17** Uhr möglich.

[Zurück](#)

Abbildung 16: Fehlermeldung bei zu häufigem Start des Selbsttests

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

ID	Timestamp	Level	Code	Message	Status
484	2019-11-21T15:34:42+01:00	INFO	1	fbc	Selbsttest erfolgreich durchgeführt.

Abbildung 17: Beispiel eines Log-Eintrags bei erfolgreichem Selbsttest

Einige der im Zuge des Selbsttest möglichen Fehler versetzen den CASA in den Soft Lock-Down Mode (siehe Kapitel 8 „Fehlerbehebung“ / Seite 41). 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 46 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 Tarifierungsfälle (TAF).

aktive TAFs					
Name	TAF-ID	Messpunktbezeichnung	Gültig ab:	Gültig bis:	Messwertliste
taf2	0a01454d480000000001.taf2.sm	DE00000000000000000000000000000000	2022-06-17 12:00:00	2025-11-04 20:30:00	Öffnen
taf2	0a01454d480000000002.taf2.sm	DE00000000000000000000000000000000	2022-06-17 12:00:00	2025-11-04 20:30:00	Öffnen
TAF7	0a01454d480000000001-taf7-2.sm	DE00000000000000000000000000000001	2022-06-17 12:00:00	-	Öffnen
taf14	taf14	DE00000000000000000000000000000000	2022-06-17 11:20:00	-	Öffnen
taf14	taf14	DE00000000000000000000000000000000	2022-06-17 11:20:00	-	Öffnen

archivierte TAFs					
Name	TAF-ID	Messpunktbezeichnung	Gültig ab:	Gültig bis:	Messwertliste
TAF7	0a01454d480000000002-taf7-2.sm	DE00000000000000000000000000000001	2022-06-17 12:00:00	2022-06-27 12:00:00	Öffnen

Abbildung 18: Beispielhafte Darstellung der vorhandenen Tarifierungsfälle (TAF)

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

Abrechnungszeiträume:			
Von:	Bis:		
2022-06-27 13:30:01	2022-06-27 14:30:00	Öffnen	
2022-06-27 12:30:01	2022-06-27 13:30:00	Öffnen	
2022-06-27 11:30:01	2022-06-27 12:30:00	Öffnen	
2022-06-27 10:30:01	2022-06-27 11:30:00	Öffnen	
2022-06-27 09:30:01	2022-06-27 10:30:00	Öffnen	
2022-06-27 08:30:01	2022-06-27 09:30:00	Öffnen	
2022-06-27 07:30:01	2022-06-27 08:30:00	Öffnen	
2022-06-27 06:30:01	2022-06-27 07:30:00	Öffnen	
2022-06-27 05:30:01	2022-06-27 06:30:00	Öffnen	

Abbildung 19: 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.

The screenshot shows the EMH metering user interface. At the top, there is a navigation bar with the logo and links for 'Startseite', 'Benutzerlog', 'Messwertliste', and 'Abmelden'. Below this, the selected billing period is '2022-06-27 13:30:01 bis 2022-06-27 14:30:00'. There are buttons for 'Download' and 'JSON'. A text block explains that the table shows measurement values for the selected period. Below this, there are footnotes defining 'Zeitstempel', 'Registrierzeitpunkt', and 'Versandt'. The main data table is as follows:

Zeitstempel	Registrierzeitpunkt	0100010800ff (kWh) ¹	0100020800ff (kWh) ¹	Versandt	Status
2022-06-27 14:30:00	2022-06-27 14:30:00	23.161,357000	22.489,143000	✓	Ok
2022-06-27 14:15:00	2022-06-27 14:15:00	23.160,457000	22.488,243000	✓	Ok
2022-06-27 14:00:00	2022-06-27 14:00:00	23.159,557000	22.487,343000	✓	Ok
2022-06-27 13:45:00	2022-06-27 13:45:00	23.158,657000	22.486,443000	✓	Ok

Abbildung 20: 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.



Um die Zählerdaten des gewählten Abrechnungszeitraums im JSON-Format im Browser anzuzeigen, gehen Sie wie folgt vor:

7. Klicken Sie auf **JSON**.

7.6 Fehlerzustand



Im Falle eines Fehlerzustands (Soft Lock-Down Mode, siehe Kapitel 8 „Fehlerbehebung“ / Seite 41) 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:

The screenshot shows the EMH metering user interface with a green header 'CASA-Benutzer-Portal'. Below the header, a white box contains the error message: 'Zurzeit leider kein Zugriff möglich. Der Gateway-Administrator wurde bereits informiert.'

Abbildung 21: Fehlermeldung im Soft Lock-Down Mode

7.7 Nachvollziehen der Tarifierung und Abrechnung

Entsprechend der Vorgaben des Mess- und Eichrechts muss dem Letztverbraucher das Nachvollziehen seiner Abrechnung ermöglicht werden.

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>

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 36) vermerkt, per Webseite angezeigt (siehe Kapitel 7.6 „Fehlerzustand“ / Seite 39) oder an den LEDs signalisiert (siehe Kapitel 2.3.2 „LEDs an der Frontseite“ / Seite 16).



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



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



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

- der CASA im laufenden Betrieb einen Integritätsfehler der Firmware festgestellt hat, den Gateway-Administrator (GWA) informiert 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	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.

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 Operative Betriebsbereitschaft

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

9.3.4 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].

9.3.5 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]

9.3.6 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 Erstaulesung 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.

9.3.7 Funktionsüberprüfung

event_id	event_sub_id	Log Level	Text der Meldung
19001	1	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	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 Eichlogs ist erschöpft. Das Gerät muss ausgetauscht werden.
4294948294	1	warning	Consumerlog für [1] ist voll. Einträge älter als 15 Monate wurden gelöscht

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

9.3.8 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.

9.3.9 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.

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 Mode“ mit einem **x** markiert sind, versetzen den CASA beim Auftreten in den Soft Lock-Down Mode.



Tritt einer der nachfolgend beschriebenen 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 Mode
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 wMBus-Modul ist nicht geöffnet	
200702	Der Kommunikationsport zum wMBus-Modul ist falsch konfiguriert	
200507	Fehler bei Kommunikation mit wMBus-Modul	
200509	Falsche Firmwareversion auf wMBus-Modul erkannt	
200504	Fehler bei Kommunikation mit wMBus-Modul	
200505	Falsche wMBus-Modulbezeichnung erkannt	
200506	Falsche Firmwareversion auf wMBus-Modul erkannt	
200710	Neustart des wMBus-Moduls nicht erfolgreich	
1800200	CLS-Socks-Server nicht gestartet	
1800201	Interne Prozesskommunikation gestört	
1800202	Kein gültiges SMGW HAN-Zertifikat (BP)	
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-Profiles 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	
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

Fehlercode	Beschreibung	Soft Lock-Down Mode
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 fehrgeschlagen	x
901000	Logout von Mobilfunkzelle: Unbekannter Fehler	
901001	Logout von Mobilfunkzelle: No Carrier	
901002	Logout von Mobilfunkzelle: DeRegistration	
901003	Logout von Mobilfunkzelle: Detach	
901004	Logout von Mobilfunkzelle: Only Emergency	
901005	Logout von Mobilfunkzelle: No Network Registration	
901006	Logout von Mobilfunkzelle: Bad Signal Strength	
901007	Logout von Mobilfunkzelle: Bad Signal Quality	
901008	Logout von Mobilfunkzelle: Bad IP Quality	
901009	Logout von Mobilfunkzelle: Missing IP-Address	
901010	Logout von Mobilfunkzelle: TX/RX Error	
901011	Logout von Mobilfunkzelle: SIM-Error	
901012	Logout von Mobilfunkzelle: Modem-Error	
901013	Logout von Mobilfunkzelle: PPP-Idle-Time	
901014	Logout von Mobilfunkzelle: Config Changed	
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 fehrgeschlagen	
2300035	Signieren der CMS-Daten fehlgeschlagen	
2300026	Kompemierung der CMS-Daten fehrgeschlagen	
2300097	Nicht ausreichend Speicher verfügbar	
2300098	Interner TLS-Fehler	
2300151	Entpacken der CMS-Daten fehlgeschlagen	
2300171	Fehlerhafte CMS-Signatur	
2300160	Verschlüsselung der CMS-Daten fehrgeschlagen	
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 Logfile gefunden, der Fehler wurde behoben	
1400002	Logdatei-Nummerierung inkonsistent	x
1400003	Logdatei-Nummerierung inkonsistent	x
1400005	Integritätscheck der Logbücher fehlgeschlagen	x

Fehlercode	Beschreibung	Soft Lock-Down Mode
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	Fehlerhaftes Dateiattribut 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
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-kodieren des Profils	
600032	interner Konfigurationsfehler	
600033	Konfigurationssynchronisation gestört	x
600034	Konfiguration setzen gestört	
600035	Konfiguration lesen gestört	
600036	Konfiguration löschen gestört	
600037	Kein Konfigurationsobject	
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

Fehlercode	Beschreibung	Soft Lock-Down Mode
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 Selbsttest 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 unbekanntem Gründen erkannt	
1900602	Es wurde ein Reboot wegen Wegfall der Versorgungsspannung erkannt	
1900603	Es wurde ein unerwartetes Rebootkommando 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	
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	

Fehlercode	Beschreibung	Soft Lock-Down Mode
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 Konfigurationsoptionen 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 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	

Fehlercode	Beschreibung	Soft Lock-Down Mode
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	
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 einen vorgegebenen Intervall keine Zeitsynchronisation 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	

Fehlercode	Beschreibung	Soft Lock-Down Mode
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 gwadient 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

[IEC 60715]	Abmessungen von Niederspannungsschaltanlagen und Geräten Standardisierte Montage auf Schienen zur mechanischen Unterstützung elektrischer Geräte in Schalt- und Geräteanlagen
[BSI-CC-PP-0073]	BSI-CC-PP-0073 „Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“, Version 1.3
[BSI-CC-PP-0077-V2-2015]	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 BSI-TR-03109 „Dachdokument“, Version 1.1
[BSI-TR-03109-1]	Technische Richtlinie BSI-TR-03109-1 „Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“, Version 1.1
[BSI-TR-03109-1-Detail-spezifikation]	Technische Richtlinie BSI-TR-03109-1 „Detailspezifikation“, 2021-09-17
[FNN-Lastenheft Logmeldungen]	FNN-Hinweis „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 und CASA 1.1 – SMGw-Schnittstellenbeschreibung (CASA API), Version 2.01
[CASA-PHB-ST-GWA-DE]	CASA 1.0 und CASA 1.1 – Installations- und Konfigurationshandbuch für Servicetechniker und für Gateway-Administratoren, Version 1.55
[CASA-PHB-LV-DE]	CASA 1.0 und CASA 1.1 – Benutzerhandbuch für Letztverbraucher, Version 1.55
[CASA-ST]	CASA 1.0 and CASA 1.1 – Security Target (CASA-ST), Version 3.03
[CASA-PHB-MessEG-DE]	CASA – Betriebshinweise für eine mess- und eichrechtkonforme Verwendung, Ver. 1.90
[GPL]	GNU 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	36
DIN – Deutsches Institut für Normung e.V.	II
EMT – Externer Marktteilnehmer	31
EnWG – Energiewirtschaftsgesetz	17
FNN – Forum Netztechnik/Netzbetrieb im VDE	20
GPL – GNU General Public Licence	42
GPRS – General Packet Radio Service	21
GWA – Gateway-Administratoren	IV
HDLC – High-Level Data Link Control	16
HüID – Herstellerübergreifende Identifikationsnummer	12
IEC – International Electrotechnical Commission	20, 53
LED – Light emitting Diode/Leuchtdiode	20
LMN – Local Meteorological Network	20
LTE – Long Term Evolution	21
MSB – Messstellenbetreiber	IV
OBIS – Object Identification System	17
OMS – Open Metering System	20
PIN – Personal Identification Number	33
PKI – Public Key Infrastructure	26
PTB – Physikalisch-technische Bundesanstalt	11
Root-CA – Root Certification Authority	26
SHA – Secure Hash	10
SIM – Subscriber Identity Module	12, 13
SMGW – Smart Meter Gateway	53
ST – Servicetechniker	IV
TAF – Tarifenwendungsfall	17
TLS – Transport Layer Security	16
VDE – Verband der Elektrotechnik Elektronik Informationstechnik e. V.	53
WAN – Wide Area Network	11
WAN-A – Wide Area Network-Antenne	20

10 Konformitätserklärung



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

