Handbuch CONEXA 3.0 für den Letztverbraucher

CONEXA 3.0 Smart Meter Gateway

Version: 2.12.1
Datum: 06.11.2024

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

A Einleitung

A-1 Infos zum Handbuch

Dieses Handbuch ist Teil der Gerätedokumentation. Es enthält die notwendigen Konfigurationsinformationen für das SMGW CONEXA 3.0 (TOE Version 1.6).

- Lesen Sie diese Anleitung vor Beginn aller Arbeiten aufmerksam durch, um Personen- und Sachschäden zu vermeiden. Bewahren Sie diese Anleitung sowie alle anderen mitgelieferten Unterlagen sorgfältig auf, damit sie während der gesamten Lebensdauer des Gerätes zur Verfügung stehen.
- Beachten Sie bei der Bedienung des Smart Meter Gateways (SMGW) unbedingt alle Dokumente.
- Wird im Dokument die Bezeichnung Hersteller verwendet, so ist damit die Theben Smart Energy GmbH gemeint.

A-2 Copyright

A-3 Softwarelizenz

ⓘ Die Software ist urheberrechtlich geschützt. Die Software wird vertrieben durch die Theben Smart Energy GmbH, Schlossfeld 9, 72401 Haigerloch. In diesem Produkt kommt Open-Source-Software (OSS) zum Einsatz. Eine Aufstellung der verwendeten OSS-Komponenten sowie deren Lizenzart und Version der Lizenz finden Sie unter https://smart-metering-theben.de/cx-lizenzen

Die Software unterliegt der Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Common Criteria (CC) Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (SMGW PP).

Das Schutzprofil wurde in der Version 1.3 unter der Zertifizierungsnummer BSI-DSZ-CC-0918 ebenfalls vom BSI zertifiziert. Entsprechend den Forderungen aus

[1] enthält das SMGW ein, nach dem Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (Security Module PP) zertifiziertes Sicherheitsmodul.

Das Schutzprofil des Sicherheitsmoduls wurde in der Version 1.03 unter der Zertifizierungsnummer [2] vom BSI zertifiziert.

A-4 Erklärung der Warnhinweise

Warnhinweise in dieser Anleitung kennzeichnen sicherheitsrelevante Informationen. Sie finden Warnhinweise innerhalb von Handlungsabläufen, vor einem Handlungsschritt, der eine Gefährdung für Personen oder Gegenstände enthält. Warnhinweise bestehen aus:

- dem Warnsymbol (Piktogramm),
- einem Signalwort zur Kennzeichnung der Gefahrenstufe,
- Informationen zur Gefahr sowie
- Anweisungen zur Vermeidung der Gefahr.

Warnhinweise erscheinen je nach Grad der Gefährdung in folgenden Gefahrenstufen:

 ACHTUNG

 HINWEIS

A-5 Kennzeichnungen und Symbole

Zur Hervorhebung von Handlungsanweisungen, Resultaten und anderen Elementen werden in den folgenden Kapiteln die hier beschriebenen Kennzeichnungen und Symbole verwendet:

- Menünamen, Formatnamen oder andere feste Bezeichnungen sind fett gekennzeichnet z.B. **ADMIN-Service**
- Handlungsabläufe sind mit ➢ gekennzeichnet:
  z.B. „➢ Kabel einstecken.“
- Resultate sind mit → gekennzeichnet:
  z.B. „→ LED leuchtet.“
- Verweise auf das Literaturverzeichnis werden mit [...] gekennzeichnet.

A-6 Allgemeine Sicherheitshinweise

Folgende Hinweise beachten:

 Alle beiliegenden Anleitungen und Informationen beachten.

Sollten diese nicht beigefügt sein, können diese beim GWH heruntergeladen werden.

Siehe Kapitel A-9 Download der Hersteller Dokumente und A-10 Download der Transparenz- und Displaysoftware TRuDI

ⓘ Der GWA wird mittels des sicheren Kommunikationswegs (über den er auch über neue Software-Updates informiert wird) über neue Versionen der Benutzerhandbücher informiert. Er verteilt die entsprechenden Dokumente an jede Rolle weiter. Diese Dokumente können über die GWH-Homepage heruntergeladen werden und ***müssen vom GWA*** der jeweiligen Rolle (EMT, Service-Techniker, Letztverbraucher) zur Verfügung gestellt werden.

 Warnungen am Gerät und in den Dokumenten beachten.

 Gerät nur in technisch einwandfreiem Zustand und ausschließlich im Sinne der bestimmungsgemäßen Verwendung betreiben.

 Das Gerät nicht außerhalb der spezifizierten technischen Daten betreiben.

 Wartungs- und Gewährleistungshinweise beachten.

A-7 Zielgruppe dieses Dokuments

Das „Handbuch CONEXA 3.0 für den Letztverbraucher" wendet sich in an den Letztverbraucher.

Der Letztverbraucher ist eine natürliche oder juristische Person, welche elektrische Energie, Gas, Wasser oder Wärme bezieht bzw. mittels eines lokalen, dezentralen Erzeugers produziert. Der Letztverbraucher ist Eigentümer der im SMGW verarbeiteten und gespeicherten Messwerte. Er kann diese an der HAN-Schnittstelle abrufen.

A-8 Rollen im Rahmen des Smart-Metering-Konzeptes

Die hier definierten Rollen sind Akteure im SMGW-Betrieb. In weiteren Phasen des Lebenszyklus können weitere Rollen involviert sein.

A-8.1 Letztverbraucher (Consumer)

Der Letztverbraucher (LV) ist die natürliche oder juristische Person, welche elektrische Energie, Gas, Wasser oder Wärme bezieht, bzw. mittels eines lokalen, dezentralen Erzeugers produziert. Der Letztverbraucher ist Eigentümer der im SMGW verarbeiteten und gespeicherten Messwerte. Er kann diese an einer am SMGW vorgesehenen Schnittstelle abrufen.

A-8.2 Externe Marktteilnehmer

Autorisierte externe Marktteilnehmer (EMT) sind aus Sicht des SMGW alle Teilnehmer mit Ausnahme des Smart Meter Gateway Administrators (GWA) im Weitverkehrsnetz (WAN), mit denen das SMGW eine Kommunikation zum Austausch von Daten aufnehmen kann. Hierunter fallen z.B. der Verteilnetzbetreiber (VNB), der Messstellenbetreiber (MSB), der Messdienstleister (MDL), der Lieferant (LF) und sonstige autorisierte Dienstleister.

A-8.3 Smart Meter Gateway Administrator

Der Smart Meter Gateway Administrator (GWA) ist die vertrauenswürdige Instanz, die das SMGW konfiguriert, überwacht und steuert. Er erstellt und administriert die in das SMGW eingespielten Profile zur Tarifierung, Bilanzierung und Netzzustandsdatenerhebung und führt bei Bedarf die Aktualisierung der SMGW-Software durch. Ein GWA stellt eine gesonderte Rolle im Weitverkehrsnetz dar und ist nicht als externer Marktteilnehmer zu sehen. Das SMGW stellt für die Administration eine Schnittstelle ins Weitverkehrsnetz (WAN) zur Verfügung.

A-8.4 Service-Techniker

Der Service-Techniker (SRV) kann vor Ort im Wirkbetrieb eine lokale Diagnoseschnittstelle am SMGW nutzen, um lesenden Zugriff auf das System-Logbuch und weitere Diagnosedaten zu erhalten.

A-8.5 Betreiber/Verwender

Betreiber/Verwender sind in der Regel die Eigentümer des SMGW. Hierunter fallen z.B. der Verteilnetzbetreiber (VNB) oder der Messstellenbetreiber (MSB). Ein Betreiber/Verwender kann auch ein externer Marktteilnehmer (EMT) sein.

A-9 Download der Hersteller Dokumente

In diesem Kapitel werden die Dokumente mit der Bezugsquelle für das Herunterladen (Download) zur Verfügung gestellt.

Dokumente des Herstellers	Bezugsquelle
CONEXA 3.0 Handbuch – Letztverbraucher [3]	https://theben-se.de/cx30
Logbucheinträge CONEXA 3.0 [4]	https://theben-se.de/cx30
Betriebshinweise für eine mess- und eichrechtkonforme Verwendung [5]	https://theben-se.de/cx30

Tabelle 1: Dokumente des Herstellers zum Herunterladen/Download

Für das Herunterladen der angegebenen Dokumente sind die folgenden Schritte notwendig:

- Den unter Bezugsquelle angegebenen Link im Browser eingeben und ausführen.
- In der Maske der Downloads werden die Dokumente angezeigt. Hier das gewünschte Dokument auswählen.
- Bei manchen Dokumenten erfolgt eine Weiterleitung zur Homepage „Mein Konto"
- Ein **neuer Benutzer** muss ein neues Kundenkonto anlegen:
- Es muss eine E-Mail-Adresse und ein Passwort vergeben werden
- Die Freischaltung des neuen Kontos erfolgt durch den Hersteller
- Nach der Freischaltung erfolgt eine Benachrichtigung des Benutzers via E-Mail, mit den für die Anmeldung erforderlichen Daten
- Der Benutzer kann sich nun bei „Mein Konto" mit seinen Daten anmelden
- Bereits registrierte und von dem Hersteller freigeschaltete Benutzer, können sich mit Ihrem Benutzernamen oder Ihrer E-Mail-Adresse und dem Passwort anmelden
- Bei einer erfolgreichen Anmeldung auf „Mein-Konto" werden alle zum Download bereitstehenden Dokumente angezeigt und können heruntergeladen werden.

A-10 Download der Transparenz- und Displaysoftware TRuDI

Die Transparenz- und Displaysoftware TRuDI kann direkt bei der Physikalisch-Technische Bundesanstalt (PTB) heruntergeladen werden.

Dokumente und Software der PTB	Bezugsquelle
Handbuch TRuDI und Software	https://www.ptb.de/cms/de/ptb/fachabteilungen/abt2/fb-23/ag-234/info-center-234/trudi.html

Tabelle 2 Dokumente der PTB zum Herunterladen/Download

ⓘ Beim Download der Transparenz- und Displaysoftware TRuDI und beim Handbuch für die Transparenz- und Display-Software der PTB (TRuDI) sind die Richtlinien der PTB-Homepage einzuhalten.

Zur Verwendung der Transparenz- und Displaysoftware TRuDI sind die Informationen aus Kapitel E-1 notwendig.

B Gerätebeschreibung

B-1 Beschreibung des Produkts

ⓘ Das SMGW ist eine eichrechtskonforme Zusatzeinrichtung für Zähler

Mit dem SMGW bietet die Theben Smart Energy GmbH eine Lösung für die Anforderungen, die im Sinne des Smart-Metering-Konzeptes zu erfüllen sind.

Hardware- und Softwarekomponenten werden so kombiniert und konfiguriert, dass alle Zählerdaten den Anforderungen entsprechend registriert, gespeichert, an berechtigte Marktteilnehmer (EMT) weitergeleitet und somit für Messdatenbereitstellung sowie Abrechnungszwecke bereitgestellt werden.

Das SMGW erhält von verschiedenen Zählern (z.B. Strom-, Gas-, Wasserzähler) die gemessenen Werte (z.B. Zählerstände, Leistung, Arbeit). Die Messwerte werden eichtechnisch korrekt gesammelt und an berechtigte Marktteilnehmer im Weitverkehrsnetz (WAN) versendet.

Zusätzlich bietet das SMGW die Möglichkeit des Aufbaus eines transparenten Kanals zwischen CLS-Komponenten (Controllable Local System) im HAN und dem EMT im WAN um z.B. Steuerungen vorzunehmen.

Des Weiteren können Letztverbraucher bzw. Service-Techniker über die HAN-Schnittstelle Verbrauchsdaten bzw. Systeminformationen abrufen.

B-2 Technische Daten

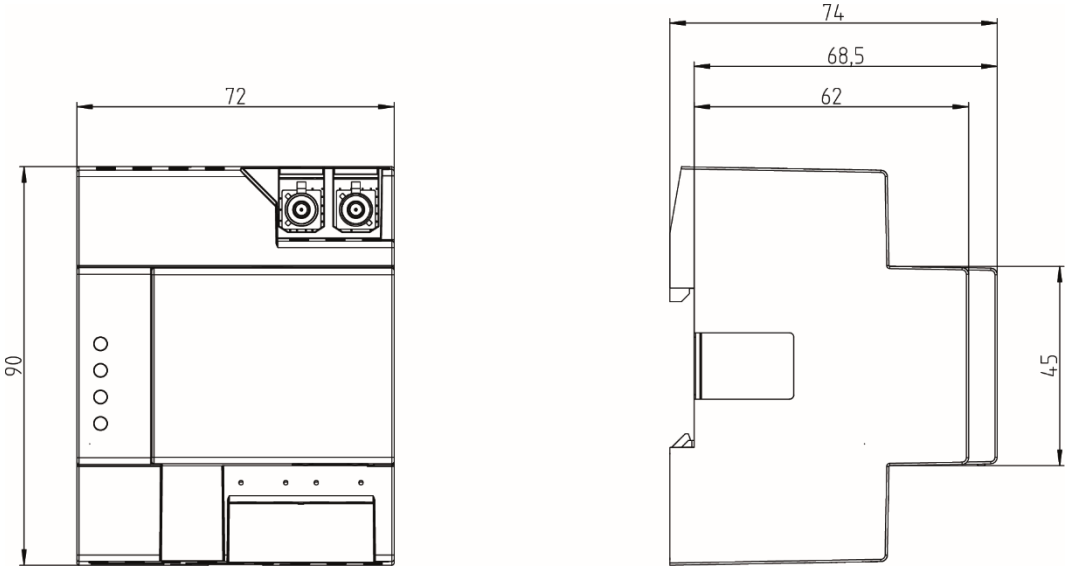

Abbildung 1: Bemaßung SMGW

Betriebsspannung:	erweiterter Betriebsbereich 230 V AC −20 % +15 %
Frequenz:	50 Hz
Stromverbrauch:	max. 0,07 A
Festgelegter Betriebsbereich:	−10 °C bis +45 °C
Grenzbereich für den Betrieb:	−25 °C bis +55 °C
Grenzbereich für Lagerung:	−25 °C bis +45 °C
Grenzbereich für Transport:	−25 °C bis +70 °C
Luftfeuchtigkeit:	95 %, nicht kondensierend
Schutzklasse:	II bei bestimmungsgemäßer Montage
Schutzart:	IP 30 nach [6] Um den nach [7] Abs. 5.9 geforderten Schutz gegen Eindringen von Staub und Wasser zu erreichen, dürfen die Geräte nur in Einbausituationen verwendet werden, die die Schutzart IP 51 erfüllen.
Brandeigenschaft	gemäß [8], Kunststoffe gemäß UL94
LMN-Schnittstelle Ausgangsspannung: Max. Strombelastung: Protokoll: Stecker:	 12 V 300 mA [9] RJ-12

Tabelle 3: Technische Daten

B-3 Anzeigeelemente und Anschlüsse

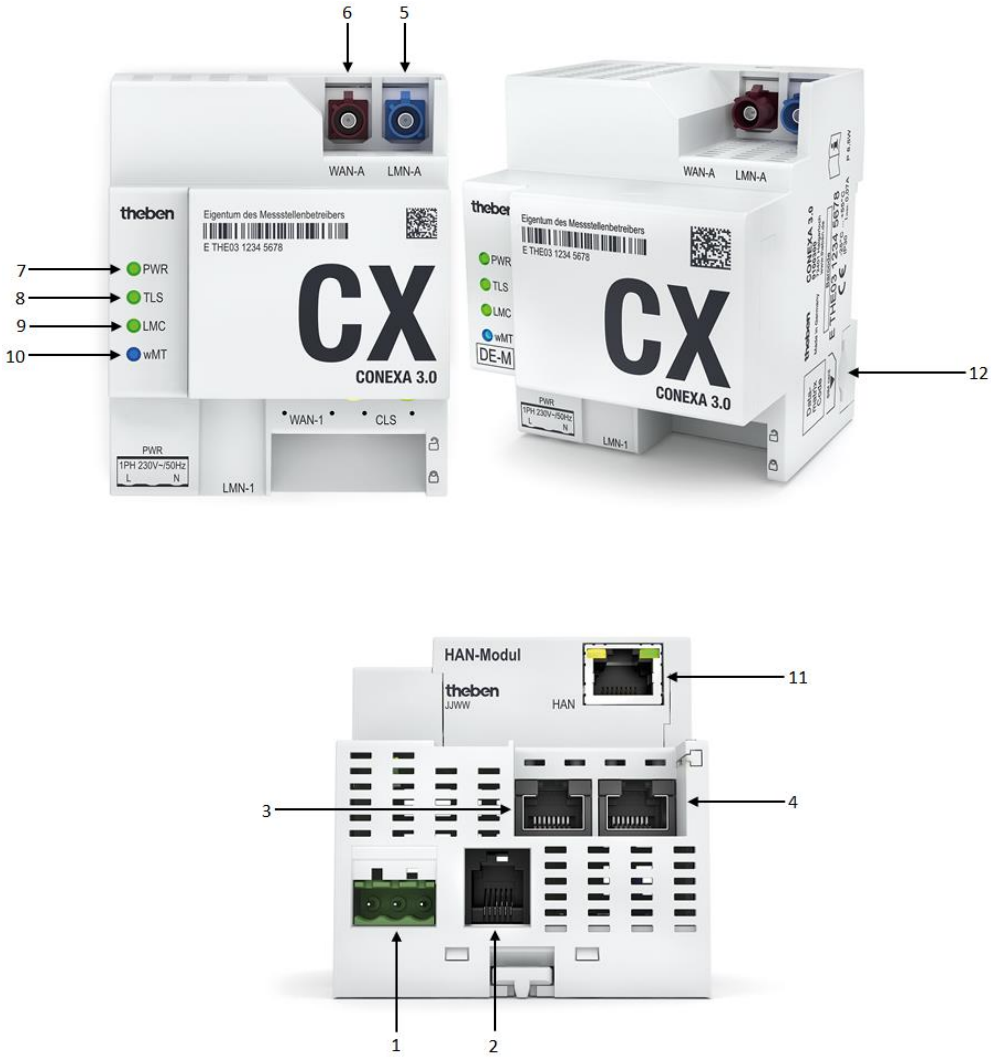

Abbildung 2: Bedienelemente und Anschlüsse

Nr.	Beschriftung	Beschreibung
1*	PWR	Spannungsversorgung 230 V (2 polig)
2*	LMN-1	Bedrahteter LMN Anschluss (RJ12)
3*	WAN-1	Ethernet Anschluss für WAN (RJ45)
4*	[HAN]CLS	Ethernet Anschluss für [HAN]CLS (RJ45)
5*	LMN-A	Antennenanschluss für unbedrahtete Zähler im LMN (FAKRA C-Codiert)

Nr.	Beschriftung	Beschreibung
6*	WAN-A	Antennenanschluss für WAN – GPRS/UMTS/LTE (FAKRA D-Codiert)
7	PWR (grün)	LED für Anzeige der Spannungsversorgung → Blinkt nach Abschluss des Bootvorgangs mit einer Impulsbreite von 500 ms. → Leuchtet dauerhaft, wenn die physikalische Betriebsbereitschaft hergestellt ist (Normalbetrieb). → Blinkt im 50ms-Takt, wenn sich das SMGW im Secure State Application oder im Secure State Boot befindet.
8	TLS (grün)	LED für die Anzeige einer bestehenden TLS-Verbindung zum GWA → Blinkt mit Beginn des Aufbaus des TLS-Kanals zum GWA mit einer Impulsbreite von 250 ms. → Blinkt weiter mit einer Impulsbreite von 250 ms, wenn der TLS-Kanal mit den Gütesiegelzertifikaten zum GWA aufgebaut wurde. → Leuchtet dauerhaft nach Wechsel der Gütesiegelzertifikate durch Wirkzertifikate durch den GWA. → Erlischt, wenn der TLS-Kanal zum GWA nicht mehr besteht. → Blinkt bei eintreffendem gültigem *Wake-Up-Paket* für eine Dauer von 3 Sekunden in einer Impulsbreite von 125 ms. Anschließend wechselt die LED in die hier beschriebenen Zustände. → Blinkt im 50ms-Takt, wenn sich das SMGW im Secure State Boot befindet.
9	LMC (grün)	LED für die Anzeige eines verbundenen drahtgebundenen Zählers → leuchtet dauerhaft, wenn für mindestens einen Zähler im LMN eine HDLC-Adresse (high level link control) vergeben und das SMGW mit der gesetzlichen Zeit vom NTP des GWAs synchronisiert wurde. → Blinkt im 50ms-Takt, wenn sich das SMGW im Secure State Boot befindet
10	wMT (blau)	LED zur Anzeige eines empfangenen Funktelegramms → Die LED bleibt für 500 ms (+/- 250ms) aktiv, wenn ein vollständiges wM-Bus-Paket empfangen wurde. → Blinkt im 50ms-Takt, wenn sich das SMGW im Secure State Boot befindet → Statusanzeige für die Signalstärke der Mobilfunkverbindung (Details siehe unten)
11	HAN	Ethernet Anschluss für HAN im kundenzugänglichen Bereich

Nr.	Beschriftung	Beschreibung
12*	SIM-Karte	Schacht für SIM Karte

Tabelle 4: Bedienelemente und Anschlüsse

ⓘ Die in der Tabelle mit * markierten Zeilen sind für den Letztverbraucher nicht sichtbar, da diese im nicht zugänglichen Bereich (unter der Abdeckung) für den Letztverbraucher sind.

Statusanzeige Mobilfunkverbindung

Beim Start des SMGW dient die wMT (blau) LED als Statusanzeige für die Mobilfunkverbindung. Zur Verdeutlichung dieser Verwendung der wMT LED leuchtet diese Dauerhaft wobei die unterschiedlichen Status (Gut/Mittel/Schlecht/kein Empfang) durch Ausschalten der LED dargestellt werden. Der Status der Mobilfunkverbindung wird für 1 Minute angezeigt. Im Anschluss wird das in Tabelle 4 beschriebene Blinkverhalten für den Empfang eines vollständigen wM-Bus-Paket angezeigt.

Die Signalstärke wird in einem Zyklus von 3 Sekunden angezeigt.

B-4 Netzwerk

B-4.1 HAN (Home Area Network)

Im HAN kommuniziert das SMGW mit dem Service-Techniker und Letztverbrauchern. Hierfür stellt das SMGW eine HAN-Schnittstelle zur Verfügung. Dieser Anschluss ist als RJ45-Buchse ausgeführt und unterstützen 10/100 MBit/s [10].

HAN: Diese Schnittstelle befindet sich auf dem Aufsteck-Modul und dient dazu, dass sich ein Letztverbraucher oder Service-Techniker im eingebauten Zustand mit dem SMGW verbinden kann.

ⓘ Die HAN-Schnittstelle **darf nicht** mit dem Internet verbunden werden. Ansonsten kann die Netztrennung zwischen WAN- und HAN-Netzwerk nicht mehr gewährleistet werden und das SMGW kann in den „Secure State Connectivity" (siehe Kapitel D-2.3) wechseln.

C Hinweise zur Verwendung des SMGW

C-1 Hinweise zur eichrechtlichen Verwendung

Für eine mess- und eichrechtkonforme Verwendung müssen die Angaben im Dokument „Betriebshinweise für eine mess- und eichrechtkonforme Verwendung" [5] beachtet und umgesetzt werden.

C-2 Bestimmungsgemäße Verwendung

Das SMGW ist ausschließlich für die Übertragung der Messdaten in Verbindung mit zugelassenen Messgeräten gemäß der technischen Beschreibung und nach ordnungsgemäßer Installation sowie mit CLS-Komponenten zu verwenden.

Zum bestimmungsgemäßen Gebrauch gehört auch die Einhaltung aller Angaben in diesem Handbuch.

Jede über den bestimmungsgemäßen Gebrauch hinausgehende Verwendung oder andersartige Benutzung gilt als Fehlgebrauch.

Hinweise zum Eichrecht

Beim SMGW handelt es sich um eine Zusatzeinrichtung für Zähler. Für Abrechnungszwecke dürfen nur eichrechtskonforme Geräte in den Verkehr gebracht und verwendet werden.

Unter Konfigurationen sind alle Parameter zu verstehen, die an die jeweiligen Bedingungen des Messstellenbetreibers angepasst werden müssen. Das sind beispielsweise Tarifeinstellungen, Einstellungen von Konfigurationsparametern zur Datenübertagung an die Datenzentrale, Mandanteneinstellungen und auch Zuordnungen von Elektrizitätszählern und Nichtelektrizitätszählern zu Mandanten. Alle Änderungen werden im Logbuch des SMGW historisch aufgezeichnet.

D Betriebszustände des SMGW

D-1 Normalbetrieb

→ Dieser Betriebszustand wird an den LEDs entsprechend Kapitel B-3 signalisiert.

In diesem Betriebszustand können sicherheitsrelevante Fehler auftreten, welche dem Benutzer zurückgemeldet werden. Diese Fehler sowie Handlungsempfehlungen sind in folgenden Dokumenten ersichtlich:

- CONEXA 3.0 Logbucheinträge [4]
- Schnittstellenbeschreibung IF_GW_CON [11]

D-2 Fehlerzustände

D-2.1 Secure State Boot

Dieser Betriebszustand tritt ein, wenn das SMGW folgende Ereignisse erkennt:

- beim Booten wird ein nicht vorhandenes oder korruptes Kernel Image oder Rootfs festgestellt,
- der Speicherbedarf für Logbücher hat die kritische Grenze erreicht,
- eine fehlerhafte inaktive Partition für Updates, welche bereits 30 Tage vorhanden ist,
- eine Abweichung der aktiven SMGW-Software-Version zur erwarteten SMGW-Software-Version feststellt.

→ Dieser Betriebszustand wird an den LEDs entsprechend Kapitel B-3 signalisiert.

Wenn der Letztverbraucher diesen Zustand feststellt muss er

➢ den zuständigen Betreiber/Verwender informieren

ⓘ In diesem Betriebszustand sind das Betriebssystem und die Applikationen nicht mehr auf dem TOE vorhanden. Jegliche SMGW Funktionalität kann nicht mehr ausgeführt werden.

D-2.2 Secure State Application

Dieser Betriebszustand tritt ein, wenn das SMGW folgende Ereignisse erkennt:

- Der Speicherbedarf für Messwerte hat die kritische Grenze (durch den GWA einstellbar) erreicht.

Oder das Zeitsystem eines der folgenden Ereignisse erkennt:

- Die Abweichung zwischen der internen Systemzeit und der verlässlichen Zeitquelle überschreitet 3% der minimalen eichtechnisch zulässigen Registrierperiode.

  → Dieser Betriebszustand wird an den LEDs entsprechend Kapitel B-3 signalisiert.

Wenn der Letztverbraucher diesen Zustand feststellt muss er

➢ den zuständigen Betreiber/Verwender informieren

ⓘ In diesem Betriebsmodus werden nur administrative Funktionen aufrechterhalten. Die weitere Funktionalität ist eingeschränkt bzw. deaktiviert.

D-2.3 Secure State Connectivity

Dieser Betriebszustand tritt ein, wenn das SMGW im Rahmen des Selbsttests folgende Ereignisse erkennt:

- Wenn im Rahmen der regelmäßigen Tests festgestellt wird, dass keine Netzwerktrennung zwischen den Netzwerken WAN und HAN vorliegt.

Im Betriebszustand „Secure State Connectivity" deaktiviert das System den Zugriff über die Schnittstellen HAN und [HAN]CLS, protokolliert das Ereignis im Systemlogbuch und benachrichtigt den GWA. Alle restlichen Funktionen des Systems bleiben weiterhin vorhanden.

ⓘ Dieser Zustand wird an den LEDs entsprechend Kapitel B-3 nicht signalisiert. Es wird ein entsprechender Systemlogeintrag geschrieben und der GWA informiert.

ⓘ Ist die HAN-Schnittstelle deaktiviert, sind die Status-LEDs der Schnittstelle aus.

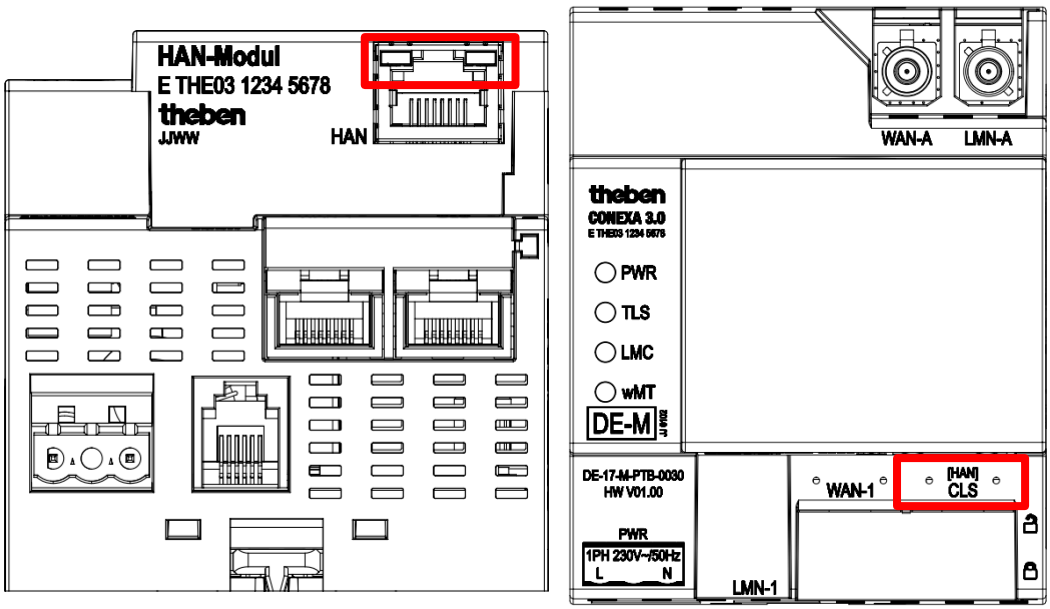

Abbildung 3: Status-LEDs der Schnittstelle an [HAN]CLS und HAN

Wenn der Letztverbraucher diesen Zustand feststellt muss er

- ➢ den Betreiber/Verwender informieren damit dieser einen Service-Techniker zur Behebung des Fehlers beauftragt.

⚠ Die Fehlerbehebung darf nur durch geschultes Elektrofachpersonal (Service-Techniker) erfolgen.

D-2.4 Secure State Measurement

Dieser Zustand tritt ein, wenn das SMGW folgende Ereignisse erkennt:

- das SMGW nimmt seine Uhrzeit als ungültig an

Wenn der Letztverbraucher diesen Zustand feststellt muss er

- den Betreiber/Verwender informieren

ⓘ Dieser Zustand wird an den LEDs entsprechend Kapitel B-3 nicht signalisiert. Es wird ein entsprechender Systemlogeintrag geschrieben und der GWA informiert.

ⓘ Messwerte, welche in diesem Zustand erfasst und abgespeichert werden, werden entsprechend markiert.

ⓘ Das SMGW verlässt diesen Zustand sobald es seine Zeit wieder als gültig annehmen kann.

D-2.5 Zyklischer Neustart des Systems

Schlagen die Sicherheitsprüfungen des Systems während des Bootvorgangs fehl führt dies dazu, dass das SMGW nicht über den Bootvorgang hinauskommt und vor dem Wechsel in den Normalbetrieb das System neu startet.

Wenn der Letztverbraucher diesen Zustand feststellt muss er

- den zuständigen Betreiber/Verwender informieren
- gegebenenfalls das SMGW ersetzen

E Aufgaben des Letztverbrauchers

Der Letztverbraucher kann über die Anzeigeelemente den Betriebszustand prüfen. Des Weiteren kann er folgenden Aktionen am SMGW ausführen:

- Auslesen der für ihn im SMGW konfigurierten Zähler-Daten
- Auslesen der Daten aus den TAFs
- Auslesen der Zählerstände und Messwertlisten
- Auslesen des Letztverbraucher-Logbuchs
- Starten des Selbsttests

Auf die oben beschriebenen Aktionen kann auf zwei unterschiedliche Arten zugegriffen werden:

1. Zugriff auf die Webseite des SMGW
    a. Zugriff auf SMGW-Informationen
    b. Ausführen des Selbsttest
2. Zugriff auf die M2M-Schnittstelle des SMGWs
    a. Zugriff auf SMGW-Informationen
    b. Zugriff auf Vertragsdaten
    c. Zugriff auf Messwerte
    d. Zugriff auf das Logbuch
    e. Ausführen des Selbsttest

Der Letztverbraucher hat je nach Konfiguration zwei Möglichkeiten zur Anmeldung an der HAN-Schnittstelle des SMGW:

1. Zugang über Benutzername und Passwort
2. Zugang über sein Schlüsselmaterial

ⓘ Die Zugangsdaten (Benutzername / Passwort oder das Schlüsselpaar) sind dem Letztverbraucher auf vertraulichem Weg vom Betreiber / Verwender zur Verfügung zu stellen.

ⓘ Das Schlüsselpaar ist mit einem Passwort geschützt.

ⓘ Zugangsdaten dürfen für Dritte nicht zugängig sein.

Das SMGW verwendet werkseitig die IP-Adresse, welche durch den Betreiber / Verwender festgelegt wurde. Diese kann durch den GWA des SMGW gesetzt und geändert werden. Der GWA kann einen dynamischen Bezug der IP-Adresse

einstellen oder eine beliebige feste IP-Adresse vergeben. Das SMGW kann der Letztverbraucher unter dieser festgelegten IP-Adresse erreichen.

ⓘ Jeder Letztverbraucher kann nur seine Daten einsehen. Die Daten von anderen Letztverbrauchern können nicht eingesehen werden.

ⓘ Die Software-Version kann vom Letztverbraucher, wie in Kapitel E-4.4.1. oder Kapitel E-5.3 beschrieben, abgerufen werden.

E-1 Bedingungen für den Zugriff des Letztverbrauchers

Es muss eine physikalische Verbindung zwischen dem SMGW und dem PC des Letztverbrauchers vorhanden sein. Die Verbindung wird über ein Ethernet-Kabel, welches an der HAN-Schnittstelle des SMGW angeschlossen sein muss, hergestellt.

Die IP-Adresse der HAN-Schnittstelle wird durch den Betreiber/Verwender zur Verfügung gestellt.

Ebenso werden die Zugangsdaten (Benutzername/Passwort oder das Schlüsselpaar) dem Letztverbraucher auf vertraulichem Weg vom Betreiber/Verwender zur Verfügung zu stellen.

ⓘ Der Letztverbraucher muss auf dem SMGW konfiguriert sein. Dies muss durch den GWA im Auftrag des Betreibers/Verwenders konfiguriert werden. Ohne diese Konfiguration ist kein Verbindungsaufbau zum SMGW möglich.

E-2 Benötigte Geräte und Tools

Hier werden die Geräte und Tools aufgeführt, welche der Letztverbraucher benötigt, um sich mit dem SMGW an der HAN-Schnittstelle zu verbinden:

- Einen PC oder ein Tablett mit einer freikonfigurierbaren Netzwerkschnittstelle (LAN), alternativ kann diese auch im Vorfeld konfiguriert werden
- IP-Adresse des SMGWs (diese wird dem Letztverbraucher durch den Betreiber/Verwender zur Verfügung gestellt)
- Einen handelsüblichen Webbrowser (z.B. Mozilla Firefox) für den Zugriff mittels Webbrowser
- Einen REST-Client zum Zugriff auf die M2M-Schnittstelle wie beispielsweise Postman (https://getpostman.com)
- Ein handelsübliches LAN-Kabel (Ethernet-Kabel)

- Eine Verbindung zwischen PC oder Tablett und SMGW muss hergestellt sein.
    - hierzu ➢Stecken Sie das Ethernet-Kabel in die freie Ethernet-Buchse am PC und in die HAN-Schnittstelle am SMGW

Die Netzwerkverbindung am PC muss gemäß E-3 konfiguriert sein.

ⓘ Alternativ zu einem REST-Client kann eine Referenzimplementierung eines Letztverbrauchertools (TRuDI) von dem Hersteller oder der Physikalisch-Technische Bundesanstalt (PTB) bezogen werden (siehe Kapitel A-10).

Die Verbindung zwischen Letztverbraucher und SMGW wird durch kryptographische Mechanismen geschützt. Hier kommt die *Transport Layer Security* (TLS) in der Version 1.2 zum Einsatz,

Alle vom Letztverbraucher zur Kommunikation mit dem SMGW verwendeten Programme müssen dieses Protokoll unterstützen.

ⓘ Die vom SMGW verwendeten Zertifikate sind selbstsigniert. Dies kann dazu führen, dass das für den Zugriff auf das SMGW verwendete Programm die Zertifikate und somit auch die Verbindung als *nicht vertrauenswürdig* einstuft. Die Zertifikate des SMGW müssen dann beim verwendeten Programm als vertrauenswürdig hinterlegt werden.

ⓘ Die maximale Sitzungslänge an der HAN-Schnittstelle beträgt 48 Stunden. Es gilt an der HAN-Schnittstelle eine maximale Leerlaufzeit von 10 Minuten. Nach überschreiten der maximalen Leerlaufzeit wird die Sitzung beendet. Es ist eine Neuanmeldung erforderlich.

E-3 Einrichten der Netzwerkverbindung am PC

Für die Kommunikation zwischen PC und SMGW müssen die Einstellungen für das Netzwerk am PC im Betriebssystem konfiguriert werden. Im Folgenden wird dies beispielhaft für das Betriebssystem Microsoft Windows 10 erläutert. Bei anderen Betriebssystemen kann dies von dem hier beschriebenen Vorgehen abweichen.

E-3.1 Einrichtung einer statischen IPv4-Adresse

E-3.1.1 Einstellungen in Windows10 öffnen

Für das Öffnen der Einstellung links unten in der Taskleiste mit der Maus auf das **Windows10-Logo** ➢klicken. Dabei öffnet sich das Start Menü (siehe Abbildung 5)

Abbildung 4: Windows Start (Win10 Logo)

Durch ➢Klicken auf das **Zahnradsymbol** im Start-Menü öffnen sich die Einstellungen (siehe Abbildung 5).

Abbildung 5: Einstellungen von Windows

E-3.1.2 Windows-Einstellungen

Es öffnet sich die Startseite für die Windows-Einstellungen. Durch das ➢Anklicken der Meldung **Netzwerk und Internet** öffnen sich die Einstellungen für den Netzwerkstatus (siehe Abbildung 6**)**

Abbildung 6: Windows-Einstellungen

E-3.1.3 Einstellungen Netzwerkstatus

In den Einstellungen **Netzwerk und Internet Status** gehen Sie jetzt mit der Maus zu dem Punkt **Netzwerk- und Freigabecenter.** Die Auswahl bestätigen Sie durch das ➢Anklicken des **Netzwerk- und Freigabecenter,** welches geöffnet wird (siehe Abbildung 8).

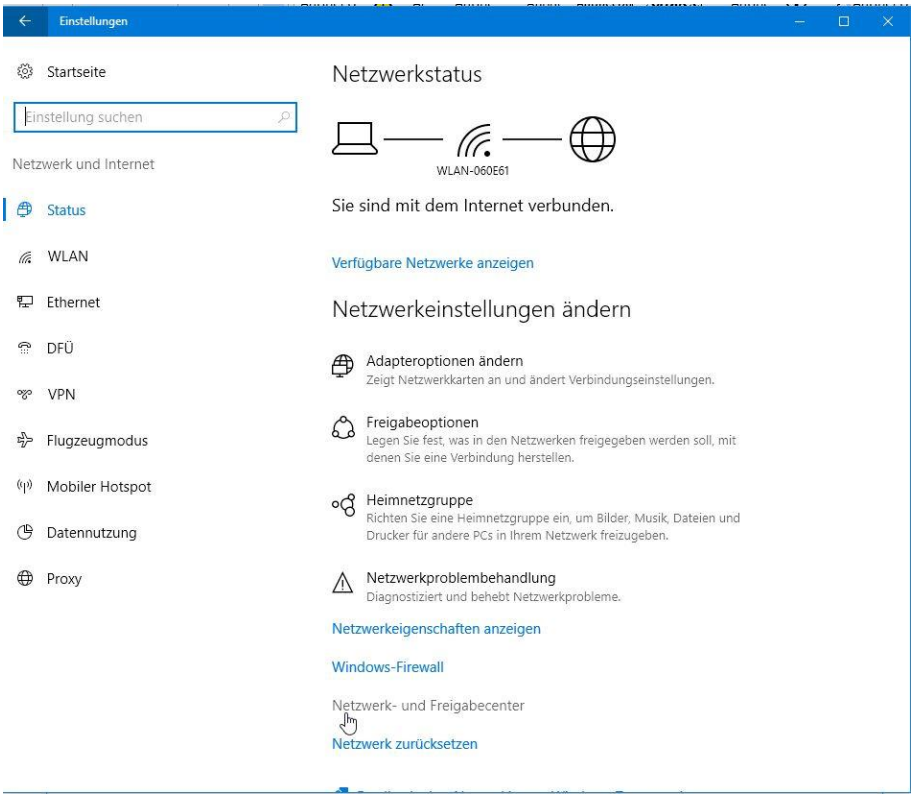

Abbildung 7: Einstellungen Netzwerkstatus

E-3.1.4 Netzwerk- und Freigabecenter

In dem geöffneten **Netzwerk- und Freigabecenter** (Abbildung 8) gehen Sie mit der Maus auf den Punkt **Adaptereinstellungen ändern.** Diese Auswahl wird durch das ➢Anklicken bestätigt und es öffnen sich die **Netzwerkverbindungen** (siehe Abbildung 9).

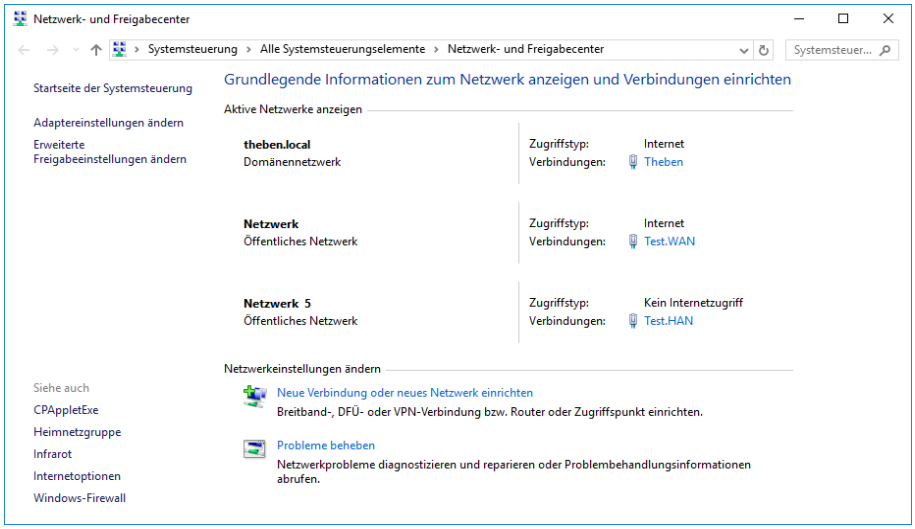

Abbildung 8: Netzwerk- und Freigabecenter

E-3.1.5 Netzwerkverbindungen

In den Netzwerkverbindungen werden alle aktiven und inaktiven Netzwerkadapter des PCs angezeigt. Jetzt gehen Sie mit der Maus auf den Netzwerkadapter bei dem die IP-Adresse eingestellt werden soll. Durch das ➢Anklicken wird die Auswahl festgelegt.

Jetzt ➢klicken Sie mit der rechten Maustaste auf den ausgewählten Netzwerkadapter (z.B.: Test.HAN). Es öffnet sich ein Kontextmenü (siehe Abbildung 10). In dem ***Kontextmenü*** gehen Sie mit der Maus auf die **Eigenschaften** und ➢klicken diese an. Es öffnen sich die **Eigenschaften des Netzwerkadapters** (Siehe Abbildung 11).

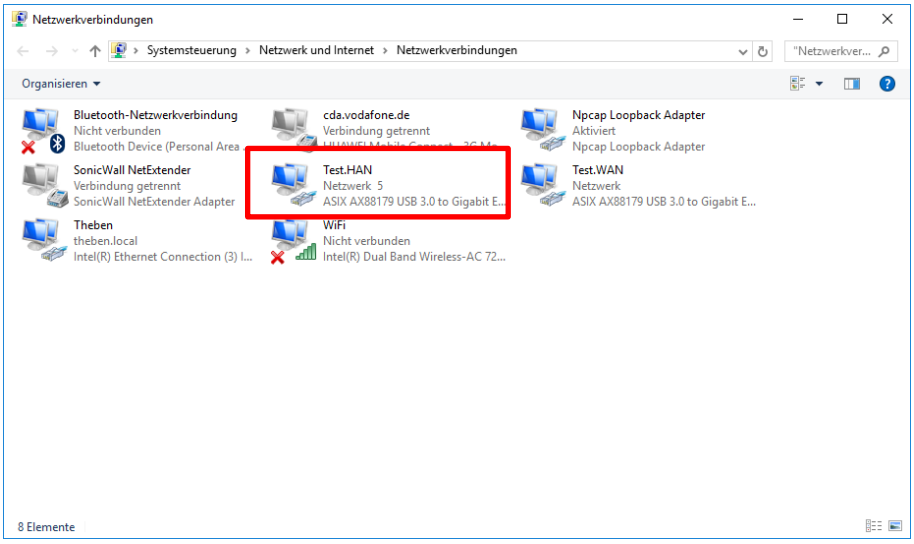

Abbildung 9: Netzwerkverbindungen

E-3.1.6 Kontextmenü

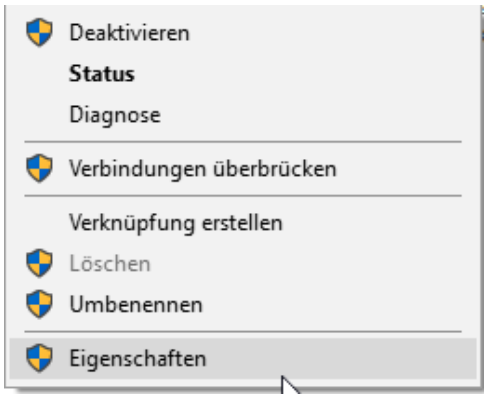

Abbildung 10: Kontextmenü

E-3.1.7 Eigenschaften des Netzwerkadapters

Die Eigenschaften des Netzwerkadapters öffnen, hier wählen Sie den Punkt **Internetprotokoll. Version4 (TCP/IPv4)** aus. (siehe Abbildung 11). Hier auf **Eigenschaften** ➢klicken. Die Eigenschaften des Netzwerkadapters werden geöffnet (siehe Abbildung 12).

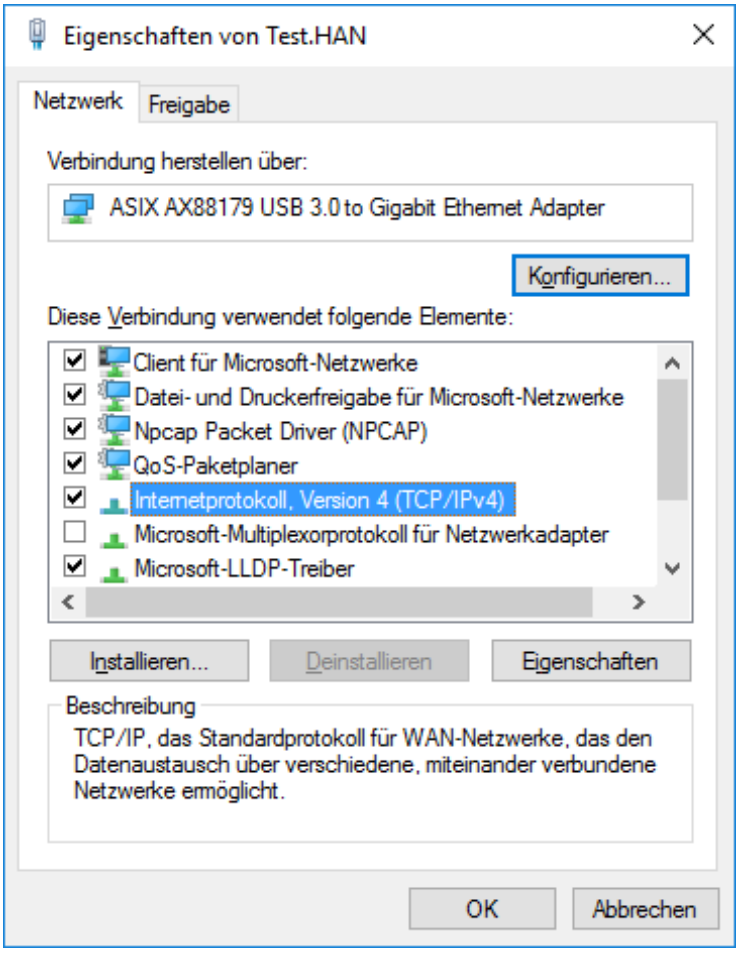

Abbildung 11: Eigenschaften von Test.HAN

E-3.1.8 Eigenschaften des Internetprotokolls, Version 4 (TCP/IPv4)

In den Eigenschaften des **Internetprotokolls, Version 4 (TCP/IPv4)** ist die Standardeinstellung **IP-Adresse automatisch beziehen**.

Um diese Einstellungen zu ändern, gehen Sie auf den Punkt **Folgende IP-Adresse verwenden:** und bestätigen die Auswahl durch ➢Anklicken**.** Nach der Auswahl können folgende Eingabefelder bearbeitet werden:

- IP-Adresse:
- Subnetzmaske: und
- Standardgateway

Nun kann die IP-Adresse, in unserem Beispiel die IP-Adresse ***192.200.1.0*** und die ***Subnetzmaske: 255.255.255.0*** eingegeben werden. Diese Informationen werden vom GWA zur Verfügung gestellt. Das Eingabefeld Standardgateway: bleibt leer (siehe Abbildung 12). Das Abschließen der Eingabe mit dem ➢OK bestätigen. Das Fenster **Internetprotokoll, Version 4 (TCP/IPv4)** wird geschlossen und der PC ist auf IPv4-Adresse eingerichtet. Es kann nun mit dem SMGW (Die IPv4-Adresse des SMGWs ist z.B. 192.200.1.100) kommuniziert werden.

ⓘ Die IP-Adresse welche in den Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4) eingegeben wird (z.B. 192.200.1.0) darf nicht der SMGW IP-Adresse (z.B. 192.200.1.100) entsprechen Die Subnetzmaske muss identisch zu der des SMGWs sein. Die IP-Adresse des SMGW sowie die Subnetzmaske werden vom GWA zur Verfügung gestellt.

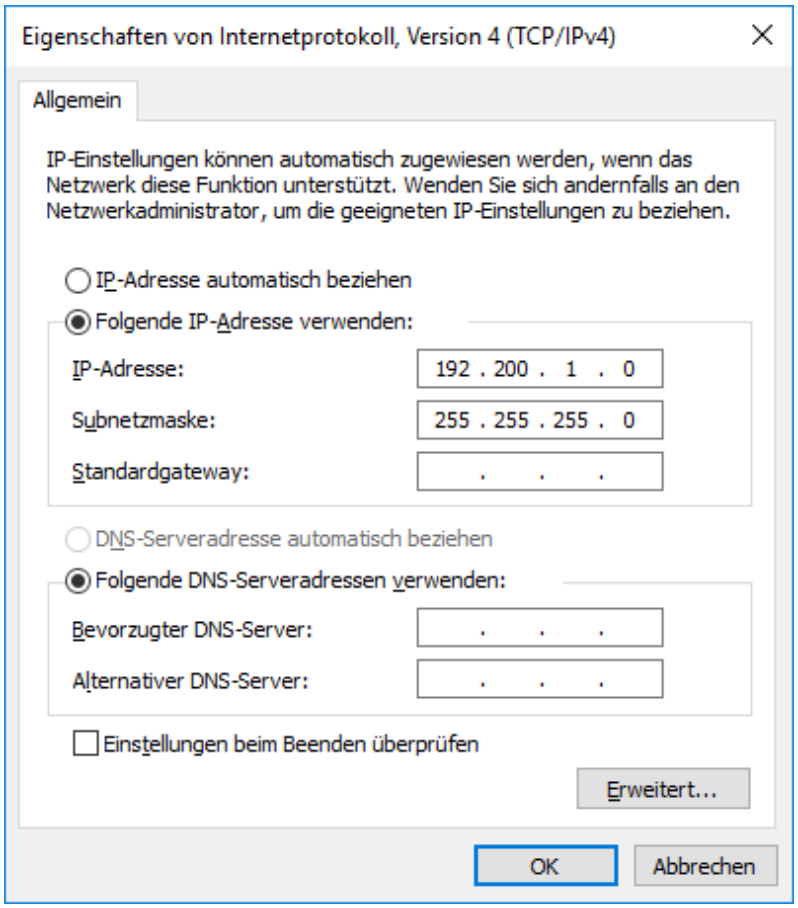

Abbildung 12: Eigenschaften des Internetprotokolls

Die geöffneten Fenster durch ➢Anklicken von OK schließen. Somit ist die Einrichtung der Netzwerkverbindung abgeschlossen.

E-4 Zugriff mittels Webbrowser

Der Letztverbraucher hat Zugriff auf Daten des SMGWs über einen handelsüblichen Internet-Browser. Die hier zur Verfügung gestellten Informationen sind stark eingeschränkt. Ein Zugriff auf alle Informationen des Letztverbrauchers bietet die sogenannte *Machine-to-Machine-Schnittstelle* (M2M-Schnittstelle) (Kapitel E-5).

Für das Beispiel wurde ein Mozilla Firefox Version 61.0.1 (64-Bit) Quantum unter Windows 10 verwendet.

E-4.1 Hinweise für den Umgang mit selbstsignierten Zertifikaten

ⓘ Die vom SMGW verwendeten Zertifikate sind selbstsigniert. Dies kann dazu führen, dass das für den Zugriff auf das SMGW verwendete Programm die Zertifikate und somit auch die Verbindung als *nicht vertrauenswürdig* einstuft. Die Zertifikate des SMGW müssen dann beim verwendeten Programm als vertrauenswürdig hinterlegt werden.

Im Folgenden sind die Prozessschritte beschrieben, wie die vom SMGW verwendeten Zertifikate als vertrauenswürdig hinterlegt zu können.

➢ Eingabe der Adresse

In der Adressleiste die URL eingeben. Hier die URL wie folgt verwenden: z.B. *https://192.200.1.1*

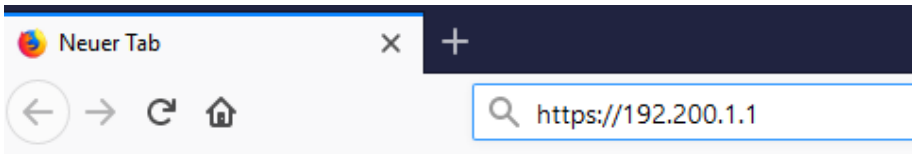

Abbildung 13: Eingabe der IP-Adresse

➢ Nicht gesicherte Verbindung

Hier wird dem Letztverbraucher angezeigt „Diese Verbindung ist nicht sicher". In dem Feld *Weitere Informationen…* auf den ➢**Button *Erweitert* klicken**. Es öffnet sich ein weiterer Dialog bei dem, dem Letztverbraucher mitgeteilt wird, dass dem Verwender nicht vertraut wird (siehe Ausnahme hinzufügen…)

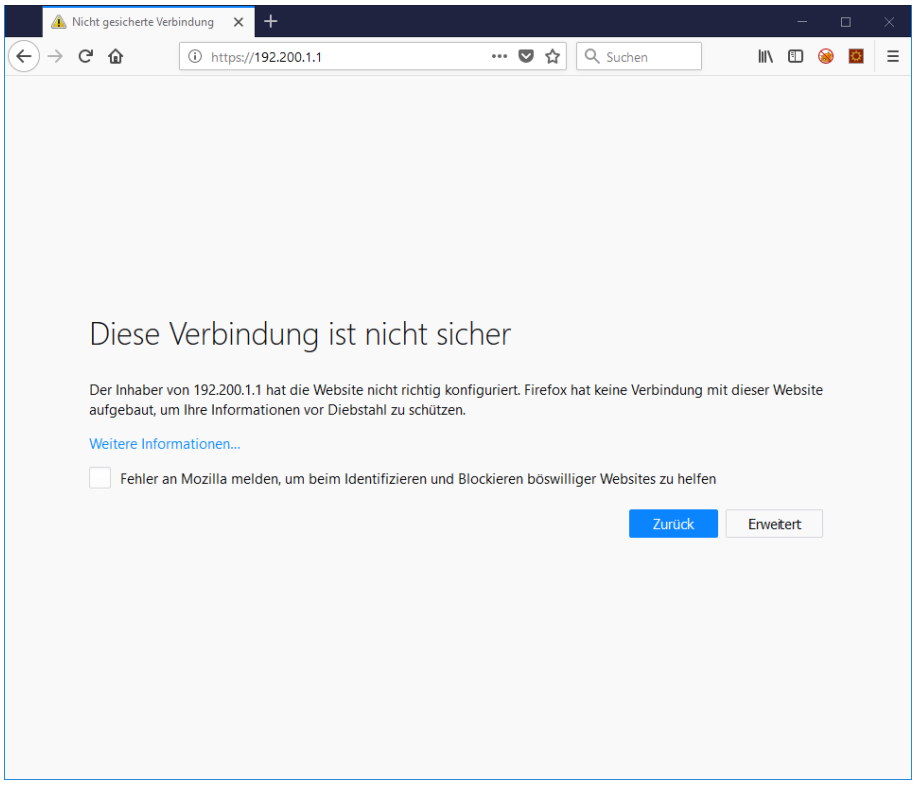

Abbildung 14: Sicherheit Information

➢ Ausnahme hinzufügen...

In der erweiterten Anzeige den ➢**Button *Ausnahme Hinzufügen*... anklicken**.

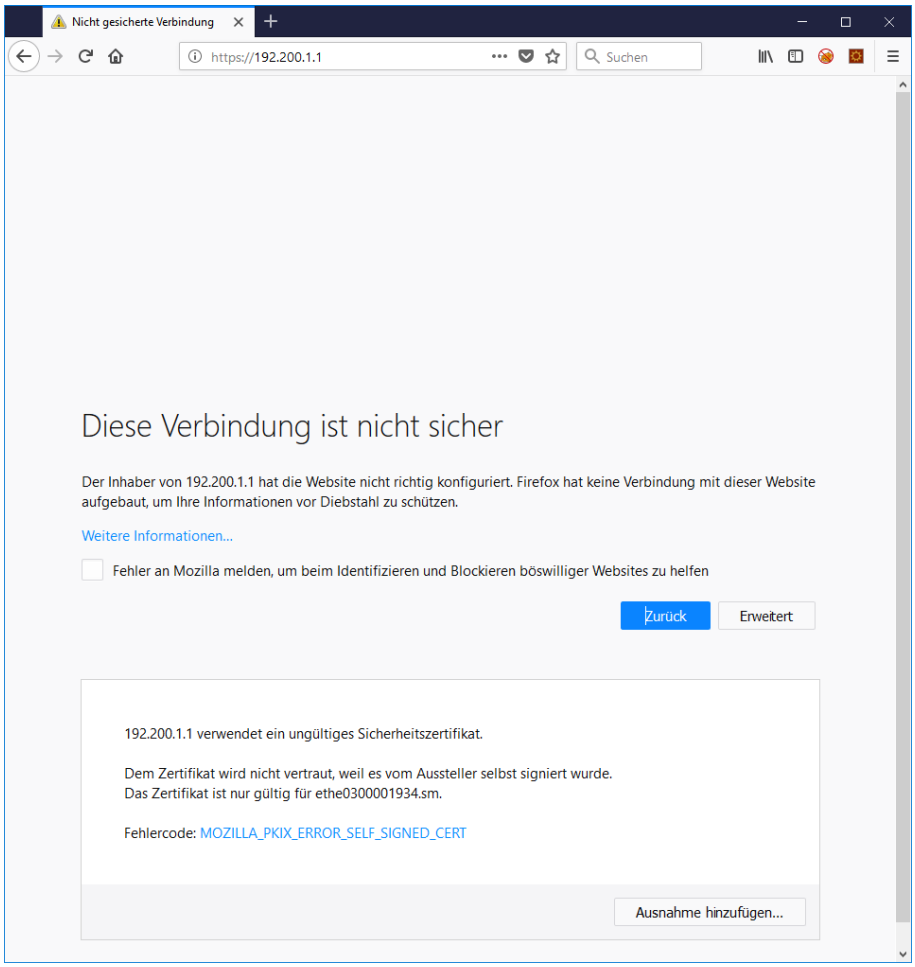

Abbildung 15: Ausnahme Hinzufügen

➢ Sicherheits-Ausnahme hinzufügen

In dem geöffneten Dialog die folgenden Schritte durchführen:

- Den ➢**Button *Zertifikat herunterladen* anklicken.**
- Es öffnet sich die Nachfrage ob diese Ausnahme weiterverwendet werden soll. Hier auf den ➢**Button *Diese Ausnahme dauerhaft speichern*** klicken. Jetzt wird die Ausnahme dauerhaft gespeichert. Im letzten Schritt muss die Sicherheits-Ausnahmeregel noch bestätigt werden.
- Zur Bestätigung der Sicherheits-Ausnahmeregel den ➢**Button *Sicherheits-Ausnahmeregel bestätigen* anklicken**. Das Zertifikat wird im Firefox hinterlegt.

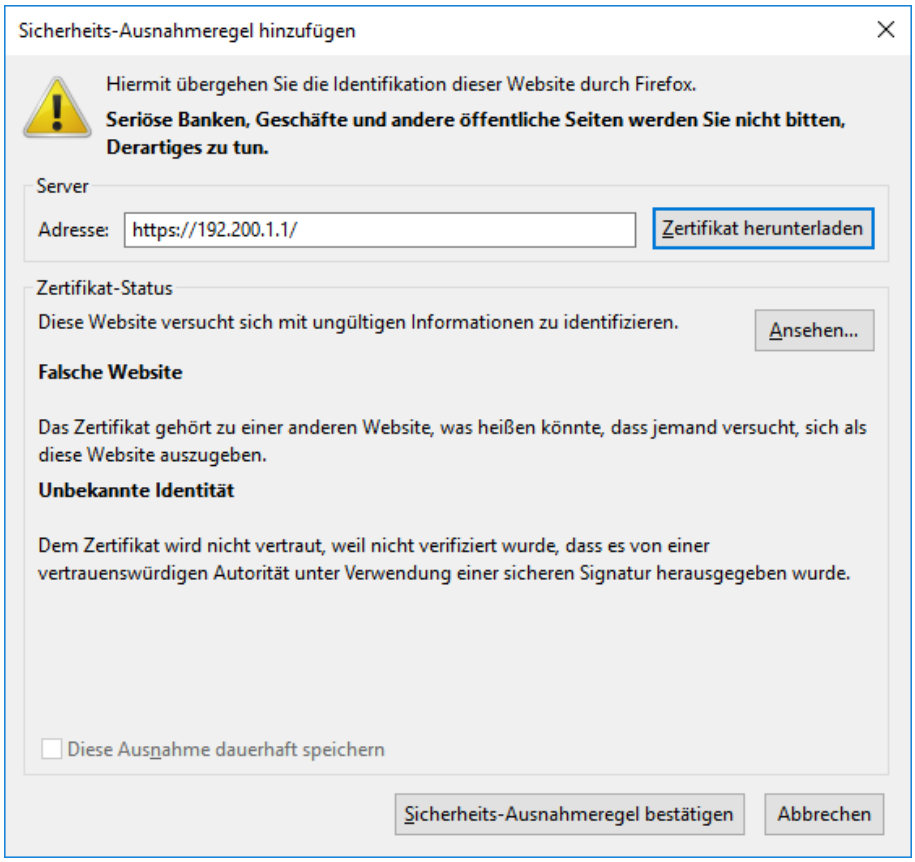

Abbildung 16: Sicherheits-Ausnahmeregel hinzufügen

E-4.2 Anmeldung mittels Schlüsselpaar

Ein Schlüsselpaar besteht aus einem öffentlichen sowie einem privaten Schlüssel. Der öffentliche Schlüssel wird in der Regel durch ein Zertifikat verteilt, welches den öffentlichen Schlüssel beinhaltet.

Für diese Anmeldung müssen die Schritte in den folgenden Unterkapiteln durchgeführt werden.

E-4.2.1 Menü öffnen / Einstellungen öffnen

Auf die drei Balken am rechten Rand des Browser ➢***Menü öffnen*** **klicken,** das Menüfenster wird geöffnet. Hier die ➢***Einstellungen*** **auswählen** und durch ➢***Anklicken*** öffnen.

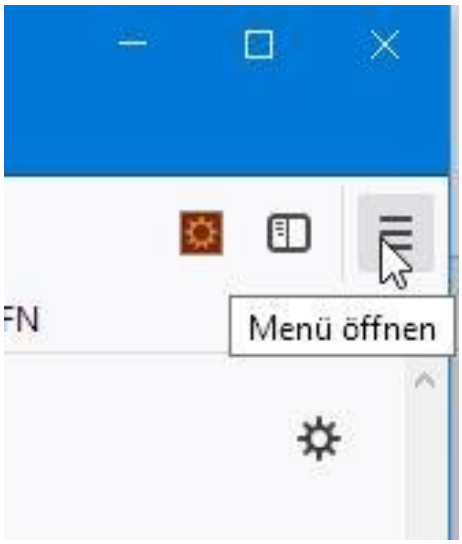

Abbildung 17 Menü öffnen

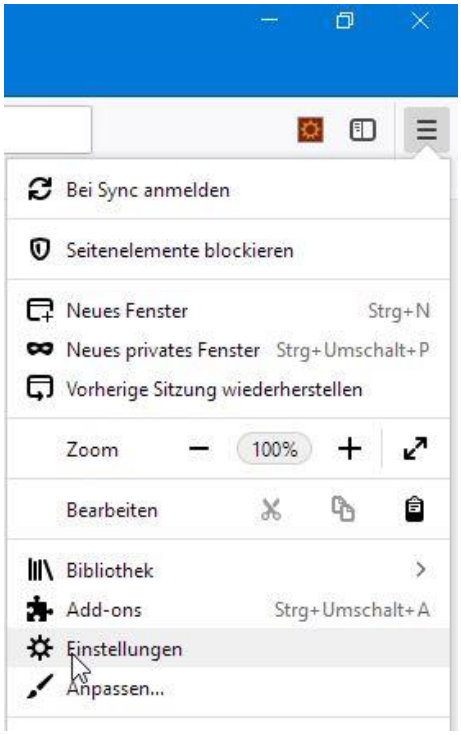

Abbildung 18: Einstellungen wählen

E-4.2.2 Einstellungen

In den Einstellungen ➢***Datenschutz & Sicherheit*** **auswählen** und durch ➢**Anklicken** die Auswahl bestätigen. Es öffnet rechts neben den Menüpunkten eine Seite beginnend mit Browser-Datenschutz.

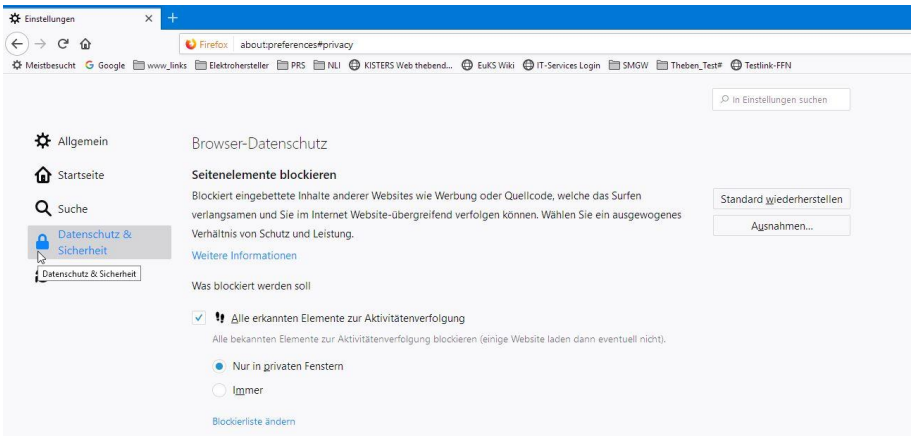

Abbildung 19: Datenschutz & Sicherheit

E-4.2.3 Datenschutz & Sicherheit

Es öffnet sich der Bereich Datenschutz & Sicherheit. Bis zum Punkt Sicherheit herunter scrollen. In der Sicherheit auf den ➢***Button Zertifikate anzeigen***... **klicken**. Es öffnet sich folgender Dialog.

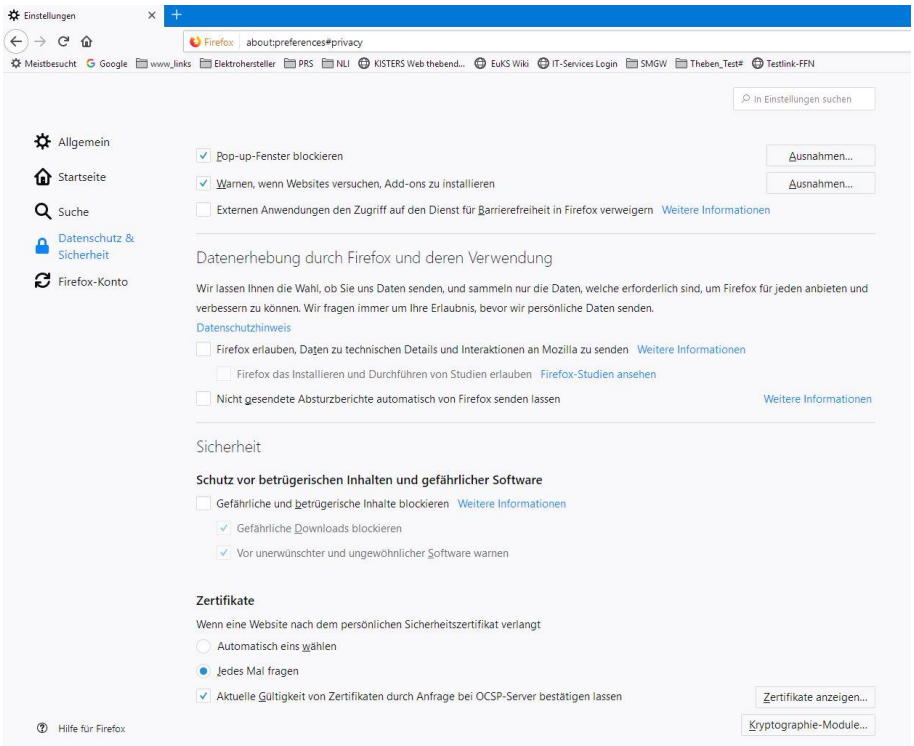

Abbildung 20: Datenschutz & Sicherheit

E-4.2.4 Zertifikatsverwaltung

Die Zertifikatsverwaltung öffnet sich. Hier auf ➢***Ihre Zertifikate*** klicken, falls dieser Dialog sich nicht automaisch öffnet. Durch ➢**Anklicken des *Buttons Importieren…*** den Importvorgang starten. Es öffnet sich folgender Dialog.

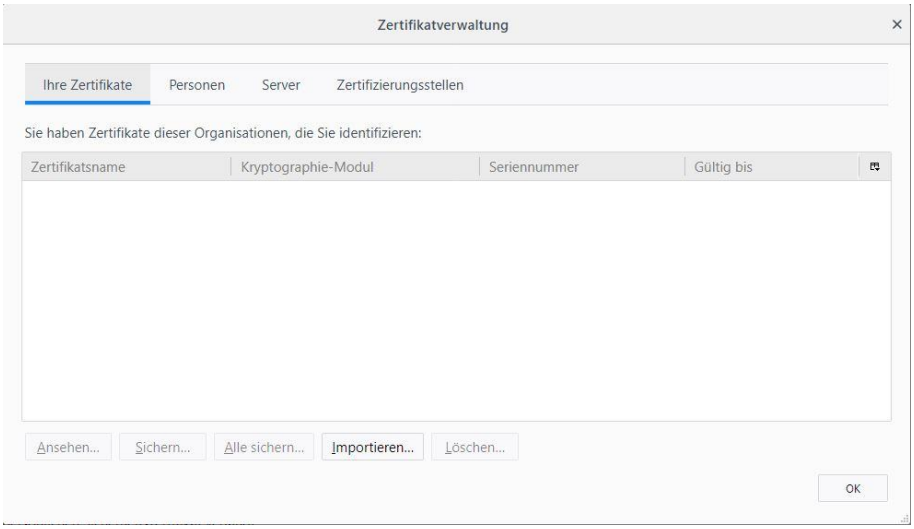

Abbildung 21: Zertifikatsverwaltung

E-4.2.5 Zu importierende Zertifikat-Datei

In dem geöffneten Dialog ***Zu importierende Zertifikat-Datei*** müssen die folgenden Schritte ausgeführt werden:

- Im linken Teil des Dialogfensters den ➢***Speicherort der Datei*** durch Anklicken auswählen und in den ➢***Ordner* wechseln,** in welchem die Zertifikats-Datei gespeichert ist.

ⓘ Das Datei-Format muss der in den Default-Einstellung PKC12-Dateien (*.p12,*.pfx) entsprechen. In diesem Datei-Format sind das Schlüsselmaterial und der Key des Letztverbrauchers enthalten. Diese Daten müssen dem Letztverbraucher durch seinen Betreiber/Verwender auf vertraulichem Weg mitgeteilt werden.

- Die gewünschte Datei im rechten Teil des Dialogfensters ➢**auswählen und anklicken**. Anschließend die Schlüsseldatei auswählen und durch ➢**Klick auf Öffnen** die Auswahl bestätigen.

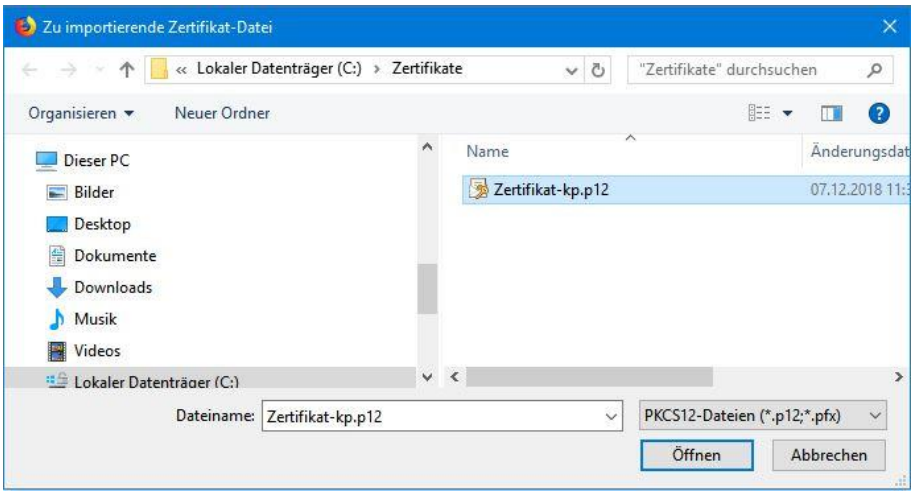

Abbildung 22: Zu importierende Zertifikat-Datei

E-4.2.6 Passwort erforderlich

Es erfolgt eine Passwortabfrage. Bei der Passwortabfrage muss der Letztverbraucher die Zertifikats-Datei durch Eingabe des Passwortes freigeben (das Passwort wird dem Letztverbraucher von seinem Betreiber/Verwender auf vertraulichem Weg mitgeteilt). Diesen Vorgang mit dem ➢**anklicken des Button *OK*** abschließen.

Erst dann wird die Zertifikats-Datei in der Zertifikatverwaltung hinterlegt.

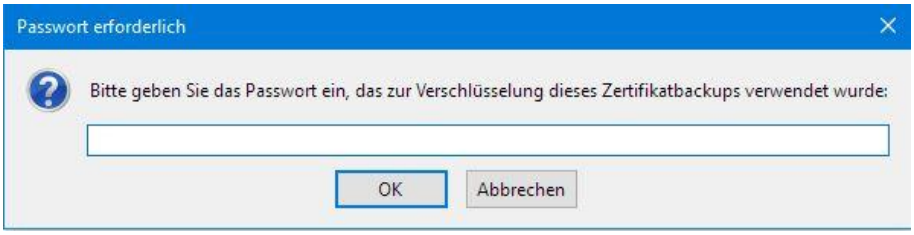

Abbildung 23: Passwort erforderlich

E-4.2.7 Zertifikatverwaltung mit Zertifikat

Nach der erfolgreichen Verifizierung der Daten mit der Eingabe des richtigen Passwortes, werden diese in der Zertifikatverwaltung angezeigt.

Das Abschließen des Imports der Zertifikate, ist durch das ➢**Klicken auf den Button *OK*** abgeschlossen und die Zertifikatverwaltung wird geschlossen.

E-4.2.8 Zugriff auf das SMGW

Um auf das SMGW zuzugreifen muss das SMGW unter dessen URL aufgerufen werden. Dies geschieht durch Eingabe des Protokolls und der IP-Adresse im Adressfeld des Webbrowsers, z.B. *https://192.200.1.1*. Anschließend leitet das

SMGW entsprechend dem angemeldeten Letztverbraucher auf dessen Startseite (Kapitel E-4.4.1) um.

E-4.3 Anmeldung mittels Benutzername und Passwort

In den folgenden Schritten wird beschrieben, wie der Webbrowser für den Zugriff des Letztverbrauchers mit seinem Benutzernamen und Passwort eingestellt/konfiguriert werden muss.

E-4.3.1 Eingabe Benutzername und Passwort

Es öffnet sich das Anmeldefenster, dass eine Authentifizierung durch den Letztverbraucher erforderlich ist.

In den Feldern „Benutzernamen" und „Passwort": Den Benutzernamen und das Passwort eingeben, welch dem Letztverbraucher durch den Betreiber/Verwender auf vertraulichem Weg zur Verfügung gestellt wurde.

Sind die Eingaben der Benutzerdaten erfolgt, kann sich der Letztverbraucher am SMGW durch das ➢**anklicken des Button *OK*** anmelden.

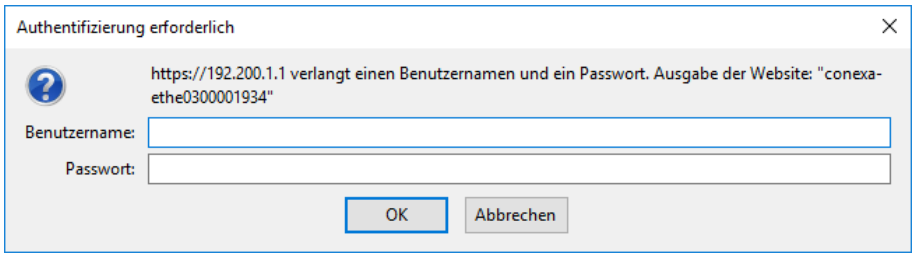

Abbildung 24: Authentifizierung erforderlich

Der Webservice des SMGWs wird gestartet siehe Kapitel

E-4.3.2 Zugriff auf das SMGW

Um auf das SMGW zuzugreifen muss das SMGW unter dessen URL aufgerufen werden. Dies geschieht durch Eingabe des Protokolls und der IP-Adresse im Adressfeld des Webbrowsers, z.B. *https://192.200.1.1*. Anschließend leitet das SMGW entsprechend dem angemeldeten Letztverbraucher auf die Startseite (Kapitel E-4.4.1) um.

E-4.4 Informationen über das SMGW

Die folgenden Operationen *Startseite*, *SMGW-Selbsttest* und *Abmelden* stehen dem Letztverbraucher auf der Startseite zur Verfügung, welche im Folgenden beschrieben werden.

E-4.4.1 Startseite

Hier werden die Informationen über das SMGW angezeigt.

Abbildung 25: Startseite

E-4.4.2 Selbsttest auslösen

➢ ***SMGW Selbsttest anklicken***. Das SMGW startet den Selbsttest.

Abbildung 26: SMGW-Selbsttest

E-4.4.3 SMGW-Selbsttest wird gestartet oder läuft

ⓘ Beim erneuten Versuch den Selbsttest zu starten, wird dies durch das SMGW unterbunden. Ein Countdown zeigt an, wann ein erneuter Selbsttest durchgeführt werden kann. Die Sperre ist auf 600 Sekunden (10 Minuten) eingestellt. Ein erneuter Selbsttest kann erst nach Ablauf der Sperre gestartet werden.

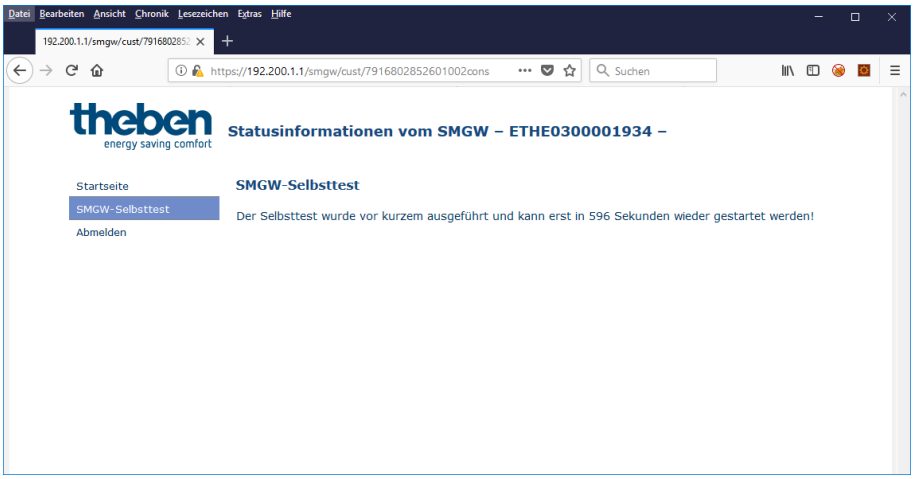

Abbildung 27: SMGW-Selbsttest läuft

E-4.4.4 Abmelden

Beim ➢***Anklicken von Abmelden***, wird die Sitzung beendet.

Abbildung 28: Abmelden erfolgreich

E-5 Zugriff auf die M2M-Schnittstelle

Über den Zugriff auf die M2M-Schnittstelle können sämtliche Informationen eines Letztverbrauchers abgerufen werden. Er bietet den Zugriff auf

- Daten des Letztverbrauchers
- Informationen über das SMGW
- Vertragsdaten des Letztverbrauchers
- Tarifierte Messwerte und
- Logdaten des Letztverbrauchers

Des Weiteren kann der Letztverbraucher manuell einen Selbsttest des Systems auslösen.

ⓘ Die zurückgelieferten Daten enthalten eichrechtlich relevante Informationen.

E-5.1 Authentifizierung des Letztverbrauchers

Die Authentifizierung des Benutzers erfolgt per *Mutual Authentication* über TLS oder durch Authentifikation per Benutzername und Passwort (HTTP-Digest) gemäß [12].

Bei der Authentifizierung des Benutzers über *Mutual Authentication* wird bei Verbindungsaufbau zunächst geprüft ob ein Client-Zertifikat übertragen wurde. Existiert in diesem Falle im Smart Meter Gateway ein zum Client-Zertifikat passendes Benutzerprofil gilt der Benutzer als authentifiziert.

Ist der Benutzer nicht gemäß *Mutual Authentication* authentifiziert erfolgt ein Rückfall auf *HTTP-Digest*, bei der der Client zur Übertragung von Benutzername und Passwort aufgefordert wird. Gibt es im Smart Meter Gateway ein zum Benutzername und Passwort passendes Benutzerprofil gilt der Benutzer als authentifiziert.

E-5.2 Zugriff auf die Root für M2M-Schnittstelle / Anmeldung

Für jeden auf dem SMGW verfügbaren Letztverbraucher wird eine separate *userid* bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist. Wird die Authentifizierung durchgeführt, so wird die Anfrage mit dem HTTP StatusCode 307 *Temporary Redirect* beantwortet. Aus dieser Antwort kann die korrekte *userid* und der *Point of Contact (POC)* für den angemeldeten Letztverbraucher entnommen werden.

Siehe hierzu [11 S. Kapitel A-2.1.]

E-5.3 Smart Meter Gateway Informationen über M2M-Schnittstelle

Der Letztverbraucher ist berechtigt, Informationen vom SMGW, wie bspw. die Software-Version, abzurufen. Der Abruf dieser Informationen ist in [11 S. Kapitel A-2.2.] beschrieben.

E-5.4 Vertragsdaten laden über M2M-Schnittstelle

Die für den Letztverbraucher eingespielten Vertragsdaten können, wie in [11 S. Kapitel A-2.3.] beschrieben, abgerufen werden. Hier wird eine Liste aller Tarife des Letztverbrauchers sowie die für den jeweiligen Vertrag geltenden Abrechnungsperioden zurückgeliefert.

E-5.5 Abruf von Informationen eines Vertrages über M2M-Schnittstelle

Detailinformationen eines Vertrages können, wie in [11 S. Kapitel A-2.4.] beschrieben, abgerufen werden.

E-5.6 Abruf von Logdaten über die M2M-Schnittstelle

Der Letztverbraucher ist berechtigt, Logdaten vom SMGW abzurufen. Dieses Letztverbraucherlogbuch enthält Informationen, welche für den eichrechtlich relevanten Betrieb notwendig sind.

Der Abruf des Letztverbraucherlogbuchs ist unter [11 S. Kapitel A-2.5.] beschrieben.

ⓘ Im Dokument Logbucheinträge [4] werden alle Event-Nachrichten und Einträge der einzelnen Logbücher beschrieben.

E-5.7 Abruf von Messwerten über die M2M-Schnittstelle

Der Letztverbraucher ist berechtigt, Messdaten seiner Verträge abzurufen. Dieser Abruf ist unter [11 S. Kapitel A-2.6.] beschrieben.

ⓘ Bei den Tarifanwendungsfällen TAF9, TAF10 und TAF14 speichert das SMGW keine Messwerte persistent. Daher können auch bei diesen Tarifanwendungsfällen keine Messwerte ausgelesen werden.

ⓘ Abweichend davon kann bei den Tarifanwendungsfällen TAF9, TAF10 und TAF14 die aktuellen Messwerte abgefragt werden.

E-5.8 Selbsttest auslösen

Das SMGW führt beim Systemstart sowie alle 24 Stunden selbständig einen Selbsttest durch. Alternativ kann ein Selbsttest vom Letztverbraucher manuell gestartet werden.

Das manuelle Starten des Selbsttests ist in [11 S. Kapitel A-2.7.] beschrieben. Die Ergebnisse des Selbsttests werden im Letztverbraucherlogbuch protokolliert. Der Abruf des Letztverbraucherlogbuchs ist in Kapitel E-5.6 beschrieben.

E-6 Prüfen des Betriebszustand

Der Letztverbraucher kann gemäß den Anzeigeelementen (Kapitel B-3) den Betriebszustand gemäß Kapitel D prüfen. Stellt der Letztverbraucher einen Fehlerzustand gemäß Kapitel D-2 fest muss er entsprechend den Handlungshinweisen reagieren.

E-6.1 Sonderfunktionen

Ob und welche Sonderfunktionen aktiv sind kann dem Logbuch anhand der Logmeldung THE.19013.0 entnommen werden. Diese Logmeldung wird bei jedem Start des SMGW geschrieben. Die Details zu dieser Logmeldung können [4] entnommen werden.

E-7 Aufgaben bei der Außerbetriebnahme

Wird das SMGW außer Betrieb genommen wird der Letztverbraucher vom Betreiber/Verwender über den geplanten Termin informiert.

Zu diesem Termin muss der Letztverbraucher

- alle ihm zugeordneten Messwerte vom SMGW abrufen und archivieren sowie
- das Letztverbraucherlogbuch abrufen und archivieren.

ⓘ Eine Referenzimplementierung eines Letztverbrauchertools (TRuDI) kann beim Hersteller oder der Physikalisch-Technische Bundesanstalt (PTB) bezogen werden.

I. Abkürzungsverzeichnis

Abkürzung	Beschreibung
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLS	Controllable Local System
CMS	Cryptographic Message Syntax
CRC	Cyclic Redundancy Check
COSEM	Companion Specification for Energy Metering
DL_reference	Data Link Reference
EMT	Externe Marktteilnehmer
ERP	Enterprise Resource Planning
FQDN	Fully Qualified Domain Name (voll qualifizierter Domänenname)
GSM	Global System for Mobil
GWA	Smart Meter Gateway Administrator
GWH	Smart Meter Gateway Hersteller
HAF	HAN-Anwendungsfall
HAN	Home Area Network
HCS	Header Check Sequence
HDLC	High-Level Data Link Control
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IC	Interface Class
IP	Internet Protocol
KAF	Kommunikationsprofil
LAF	LMN-Anwendungsfall
LF	Lieferant
LMC	Local Meter Controller
LMN	Local Metrological Network
LSB	Least significant bit
LF	Lieferant
LV	Letztverbraucher (auch Consumer genannt)
M2M	Machine-to-Machine (Kommunikation zwischen zwei Endgeräten)
MAC	Message Authentication Code
MDL	Messdienstleister
MSB, MSP	Messstellenbetreiber, Metering Service Provider
OBIS COSEM	Object Identification System
PAP	Password Authentification Protocol
PKCS	Public Key Cryptography Standards
POC	Point of Contact

Abkürzung	Beschreibung
PRF	Pseudorandom Function
PTB	Physikalisch-Technische Bundesanstalt
PWR	Power
RTC	Real Time Clock, Echtzeit-Uhr
RTT	Round Trip Time
SM-PKI	Smart-Metering-Public-Key-Infrastruktur
SMGW	Smart Meter Gateway
SRV	Service-Techniker
ST	Security Target
TAF	Tarifanwendungsfall
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation = SMGW
TR	Technische Richtlinie
TRuDI	Transparenz und Display-Software der PTB
UMTS	Universal Mobile Telecommunications System
UTC	Coordinated Universal Time (koordinierte Weltzeit)
VNB	Verteilnetzbetreiber
WAF	WAN-Anwendungsfall
WAN	Weitverkehrsnetz / Wide Area Network
WKS	WAN-Kommunikationsszenario
wMT	wireless MBus-Traffic
ZA	Zeitabweichung
ZP	Zählerprofil

II. Literaturverzeichnis

[1] **BSI.** *Common Criteria Protection Profile for a Gateway for Smart Metering Systems (BSI-CC-PP-0073).* 2014.

[2] **BSI.** *Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077).* 2014.

[3] **Theben Smart Energy GmbH.** *Handbuch CONEXA 3.0 für den Letztverbraucher.*

[4] **Theben Smart Energy GmbH.** *CONEXA 3.0 Logbucheinträge.*

[5] **Theben Smart Energy GmbH.** *Conexa 3.0 Smart Meter Gateway: Betriebshinweise für eine mess- und eichrechtkonforme Verwendung.*

[6] *EN 60529:2014-09 Schutzart durch Gehäuse (IP-Code).* 2014.

[7] *EN 50470-1:2007-5 Wechselstrom-Elektrizitätszähler-Teil1:Allgemeine Anforderungen, Prüfungen und Prüfbedingungen - Messeinrichtungen (Genauigkeitsklassen A,B und C) .* 2007.

[8] *EN 62052-11 Wechselstrom-Elektrizitätszähler - Allgemeine Anforderungen, Prüfungen und Prüfbedingungen – Teil 11: Messeinrichtungen (IEC 62052-11:2003); Deutsche Fassung EN 62052-11:2003 .*

[9] **Telecommunications Industry Association (TIA).** *TIA-485: Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems.* 2012.

[10] **IEEE.** *802.3 Ethernet Working Group - IEEE Standard for Ethernet.* 2012.

[11] **Theben Smart Energy GmbH.** *Schnittstellenbeschreibung IF_GW_CON.*

[12] **Franks, J., et al., et al.** *RFC 2617: HTTP Authentication: Basic and Digest Access Authentication.* 1999.