FAQ

Funkkommunikation und Datensicherheit im Stromzählernetzwerk von Kamstrup

Dieses Dokument kann als Argumentationshilfe bei Rückfragen in Hinblick auf die Sicherheit der Funkkommunikation und Daten bei OMNIPOWER-Zählern von Kamstrup verwendet werden.

Stand September 2016

Funkkommunikation

Wie werden die Stände der Stromzähler an das Versorgungsunternehmen übermittelt?

Die Zählerstände werden per Funkkommunikation – über ein Radio Mesh Netzwerk (Funknetzwerk) auf für die Datenkommunikation vordefinierten Frequenzen – an das Versorgungsunternehmen übertragen.

Was ist Funkkommunikation?

Bei Funkkommunikation handelt es sich um eine drahtlose Kommunikationsmethode, bei der elektromagnetische Wellen, die sogenannten Radiowellen, genutzt werden, deren Frequenzbereich zwischen etwa 3 kHz und 300 GHz liegt. Der OMNIPOWER-Zähler von Kamstrup kommuniziert auf einer Frequenz von 433 bis 444 MHz.

Welche Kommunikationstechnologien setzt Kamstrup bei seinen Stromzählern ein?

Drahtloskommunikation kommt an zwei Stellen der Kamstrup-Infrastruktur zum Einsatz. Kamstrup setzt Funknetzmodule vornehmlich für die Kommunikation zwischen dem Zähler und dem Konzentrator ein. Wenn der Zähler in einer eher ländlichen Gegend eingesetzt wird oder die Funkbedingungen dies erfordern, nutzt Kamstrup auch Punkt-zu-Punkt-Kommunikation (2G/3G). .

Die Kommunikation zwischen dem Konzentrator und dem zentralen Datenerfassungssystem erfolgt üblicherweise in Form einer Punkt-zu-Punkt-Kommunikation, etwa über eine drahtgebundene IP- bzw. eine drahtlose 2G/3G-Verbindung.

Erfüllen die Funkmodule in den Stromzählern von Kamstrup die gesetzlichen Vorgaben?

Ja. Neben der Prüfung und Zulassung der Kommunikationsmodule gemäß den Anforderungen der Messgeräterichtlinie in Bezug auf Zähler werden alle Kamstrup-Funkmodule auch nach den Anforderungen der R&TTE-Richtlinie (R&TTE = Funkanlagen und Telekommunikationsendgeräte) getestet. Zu den grundlegenden Anforderungen der R&TTE-Richtlinie gehören Anforderungen zur elektrischen Sicherheit, Gesundheit, elektromagnetischen Verträglichkeit und effizienten Nutzung des Funkspektrums.

Was ist ein Funknetzwerk?

Ein Funknetzwerk ist nach dem Maschenprinzip strukturiert, bei dem alle Zähler miteinander kommunizieren und sich gegenseitig dabei unterstützen, Daten an den zentralen Konzentrator zu schicken, was üblicherweise viermal am Tag (alle 6 Stunden) erfolgt.

Bei einem Funknetzwerk handelt es sich um ein Zwei-Wege-System. Das heißt, dass die Zähler Daten an einen Konzentrator senden und auch von diesem empfangen können. Dies kann zum Beispiel bei Fehlerbehebung, Verteilungsnetzanalyse, Software-Updates der Stromzähler usw. der Fall sein.

Was ist elektromagnetische Strahlung?

Strahlung eines Zählers ist elektromagnetische Energie, die von allen aktiv stromverbrauchenden Geräten erzeugt wird. Je größer der Abstand zum Gerät, desto niedriger ist das Niveau der elektromagnetischen Strahlung.

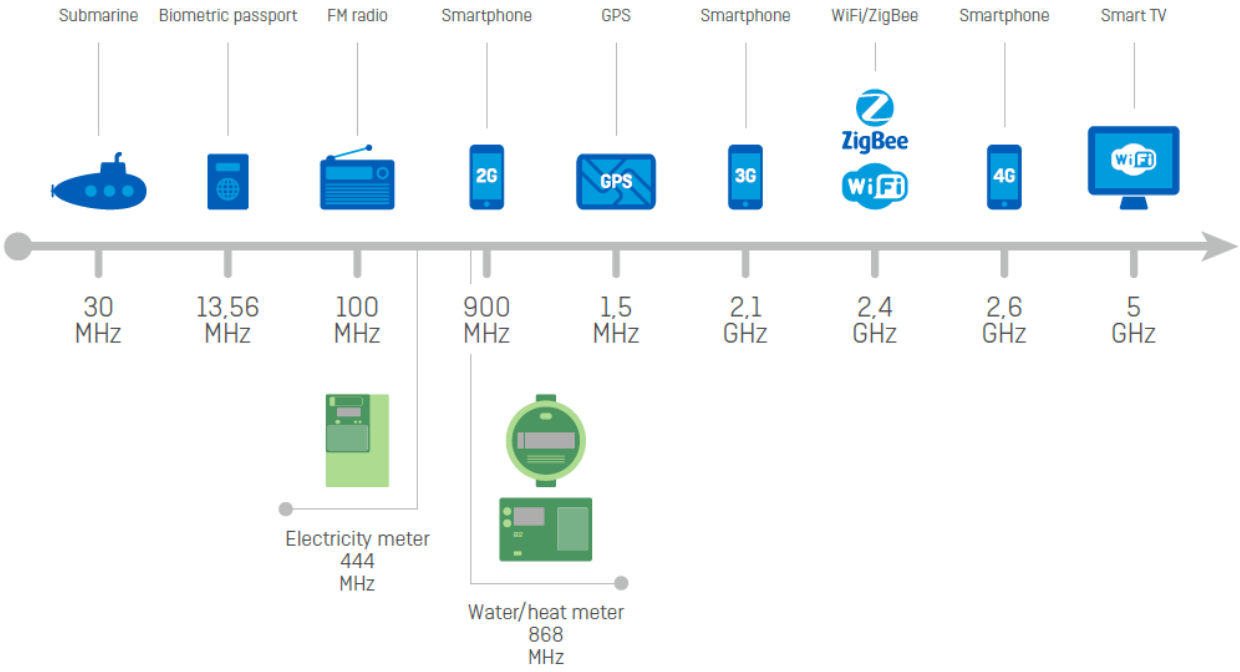
Kann ein Stromzähler elektromagnetische Strahlung erzeugen?

Da es sich bei einem Stromzähler um ein elektrisches Gerät handelt, erzeugt er elektromagnetische Strahlung. Die Grenzwerte für elektromagnetische Strahlung werden durch die unabhängige Organisation

ICNIRP (International Commission on Non-Ionizing Radiation Protection – www.icnirp.org) festgelegt. Die Organisation setzt sich aus Fachleuten aus den Bereichen Medizin und Naturwissenschaften zusammen und wird bei ihrer Arbeit von der WHO (Weltgesundheitsorganisation) unterstützt. Die Stromzähler von Kamstrup erfüllen alle nationalen Anforderungen, einschließlich der gesundheitsbezogenen Erfordernisse in Zusammenhang mit elektromagnetischer Energie.

Folgende Elektrogeräte senden ebenfalls elektromagnetische Energie aus:

- PC und WLAN
- Haushaltsgeräte
- Fernbedienungen für das Auto
- Babyphone
- Drahtlose Türklingeln, Telefone und Sensoren für Alarme und Klimaregelung



Kann man Funkkommunikation hören?
Die Funkkommunikation der Stromzähler von Kamstrup erfolgt bei Frequenzen, die 22.000 Mal höher sind als die Frequenzen, die für einen durchschnittlichen Menschen hörbar sind. Es ist naturwissenschaftlich belegt, dass Radiowellen andere Eigenschaften haben als akustische Schallwellen und daher nicht hörbar sind. Diesen Fakten entsprechend kann Funkkommunikation akustisch nicht wahrgenommen werden.

Mit welcher Leistung sendet der Stromzähler?
Die Sendeleistung des Zählers beträgt 10 bis 500 mW. Im Vergleich: Ein herkömmliches Mobiltelefon sendet mit einer Leistung von bis zu 2000 mW. Wenn der Zähler keine Daten sendet, beträgt die Sendeleistung null.

Welche EU-Richtlinien und anwendbaren Normen erfüllen die Stromzähler von Kamstrup?
In der EG-Konformitätserklärung von Kamstrup sind jene Normen aufgeführt, die für den Zähler maßgeblich sind und von ihm erfüllt werden. Kamstrup erfüllt mit seinen Produkten somit alle EU-Richtlinien und

Zulassungskriterien, die für die Zähler Voraussetzung sind. Kamstrup stellt dies vor der Markteinführung in der EU sicher. Die EU-Anforderungen werden in nationalen Gesetzen der EU-Mitgliedsstaaten umgesetzt.

Auf Anfrage stellt Kamstrup die EG-Konformitätserklärung bereit.

Wie wird die Strahlung drahtloser Geräte gemessen?

Die Strahlung drahtloser Geräte wird häufig als SAR-Wert (spezifische Absorptionsrate) angegeben. Der SAR-Wert gibt an, wie viel Energie der Körper absorbiert, wenn er elektromagnetischen Feldern ausgesetzt ist. Diese Messung wird normalerweise bei Produkten durchgeführt, die nah am Körper verwendet werden (z. B. Mobiltelefone und andere Handgeräte). Die Messung soll sicherstellen, dass der anerkannte europäische Grenzwert von 2 W/kg nicht überschritten wird. Der Abstand zwischen Sender und Körper hat einen wesentlichen Einfluss auf den SAR-Wert, d. h. je größer der Abstand, desto niedriger der SAR-Wert und somit der Einfluss auf den Körper. Ein Stromzähler befindet sich – im Gegensatz zu Mobiltelefonen – normalerweise nicht nahe am Körper.

Wo wird der Konzentrator installiert?

Der Konzentrator wird häufig in Umspannwerken oder anderen öffentlichen Orten installiert, damit das Versorgungsunternehmen einen möglichst einfachen und schnellen Zugang zum Installationsort hat.

Wie hoch ist die elektromagnetische Strahlung des Konzentrators?

2G/3G-Module von Kamstrup arbeiten mit 900/1800/2100 MHz und verfügen über eine maximale Sendeleistung von 2000 mW. Aufgrund der automatischen Regelung der Sendeleistung wird die maximale Sendeleistung in der Kamstrup-Infrastruktur nur selten erreicht.

Der SAR-Wert liegt üblicherweise zwischen 0,6 und 0,7 W/kg bei maximaler Sendeleistung und bleibt somit deutlich unter dem zulässigen europäischen Grenzwert von 2 W/kg. Die Sendeleistung der Funkmodule in den Konzentratoren beläuft sich typischerweise auf 25 % der maximalen Sendeleistung eines 2G/3G-Moduls. Der SAR-Wert der Funkmodule ist dementsprechend niedriger als 0,6 bis 0,7 W/kg.

Das elektromagnetische Feld, das bei Kamstrup Funk für den menschlichen Körper ausgeht, ist auf einer Entfernung von 20 cm bis zu 800 x schwächer als bei 2 G GSM (20 cm sind gewählt, weil es das Limit ist, um das messen zu können).

Das elektromagnetische Feld, das bei Kamstrup Funk für den menschlichen Körper ausgeht ist bei einer Entfernung von 2,5 m ungefähr 200.000 x schwächer ist als die von den Behörden auferlegte Sicherheitsgrenze.

Distanz ist immer ein nennenswerter Punkt. Der Zähler ist selten direkt beim Menschen und man hat auch den Zähler nicht bei sich wie ein Mobiltelefon. Vermutlich ist auch der Zähler nicht direkt neben den Schweinen angesiedelt – das wäre zu erforschen.

Datensicherheit

Was ist Datensicherheit?

Viele Menschen verbinden Datensicherheit mit Hackerangriffen. Auch wenn Hacker versuchen, die Datensicherheit zu untergraben, so geht es bei der Datensicherheit doch um viel mehr als nur zu verhindern, dass Hackerangriffe stattfinden.

Ein System wird in der Regel anhand dreier Aspekte auf Datensicherheit hin geprüft: Vertraulichkeit, Integritätsschutz und Verfügbarkeit.

Vertraulichkeit bedeutet, dass Sie sicher sein können, dass die Nachricht bei der Übertragung nur vom Sender und Empfänger gehört bzw. gelesen werden kann. Beispielsweise kann ein Brief vom Briefträger geöffnet und gelesen werden – eine Verletzung der Datensicherheit. Ist der Brief verschlüsselt, versteht der Briefträger die Nachricht nicht und die Vertraulichkeit bleibt gewahrt.

Integritätsschutz bedeutet, dass eine Nachricht nicht unbemerkt verändert werden kann. Ziehen wir erneut das Beispiel mit dem Briefträger heran: Der Briefträger ändert die verschlüsselte Nachricht ein wenig, sodass sie für ihn weiterhin verschlüsselt ist. Durch die Veränderung kann nun aber der Empfänger die Nachricht ebenfalls nicht mehr lesen oder versteht sie falsch. Einige Verschlüsselungscodes verfügen über Schutzmechanismen gegen diese Art von Eingriffen, sodass der Empfänger die Änderung in der Nachricht bemerkt und sich nicht auf die Zuverlässigkeit der Nachricht verlassen wird. Dies bezeichnet man als Integritätsschutz. Eine Variante des Integritätsschutzes stellt sicher, dass der Briefträger dem Empfänger nicht eine kopierte Version überbringen kann, ohne dass dieser das bemerkt.

Der dritte Aspekt ist die **Verfügbarkeit**, d. h. die Fähigkeit des Systems sicherzustellen, dass eine Nachricht immer verfügbar ist und den Empfänger erreichen kann. Dieser Aspekt hat weitreichende Auswirkungen, da die Verfügbarkeit an vielen verschiedenen Stellen und auf unterschiedlichste Weise beeinträchtigt werden kann. In unserem Briefträgerbeispiel hieße das, dass der Absender eine Kopie des Briefes behält, damit die Nachricht nicht verloren geht, selbst wenn der Briefträger den Brief wegwirft. Es bedeutet aber auch, dass der Absender zwei verschiedene Briefträger einsetzen kann, um sicherzugehen, dass die Nachricht versandt wird, auch wenn einer der Briefträger die Post nicht vorbei bringt. Ebenso bedeutet das, dass der Briefträger zwei verschiedene Fahrräder zur Verfügung hat und die Nachricht sowohl in den Briefkasten als auch in den Türschlitz des Empfängers einwerfen kann, sodass die Nachricht auch zugestellt werden kann, wenn der Briefkasten überläuft.

Einem Hacker genügt es häufig, nur einen dieser Aspekte anzugreifen. Daher konzentriert sich Kamstrup nicht nur auf einen dieser Punkte, sondern stellt sicher, dass die Datensicherheit in allen drei Aspekten gewährleistet ist.

Wenn es um Datensicherheit von fernauslesbaren Stromzählern geht, sind hauptsächlich zwei Dinge von Bedeutung: die sichere Übertragung der Stromverbrauchsmessung an das Versorgungsunternehmen sowie der Schutz des Stromzählers und des Systems vor Hackerangriffen und Übernahmen durch Dritte, was einen Kontrollverlust des Versorgungsunternehmens über diese Zähler und Systeme bedeuten würde. Die Systeme von Kamstrup sorgen dafür, dass das Versorgungsunternehmen die Kontrolle über die fernauslesbaren

Stromzähler behält und so unter anderem die Versorgung von säumigen Zahlern stoppen und nach erfolgter Zahlung wieder aufnehmen kann. Die Datensicherheit dieser Systeme gewährleistet, dass Hacker nicht die Kontrolle übernehmen können.

Wie gewährleistet Kamstrup Datensicherheit?

- Unsere Stromzähler erfüllen internationale Standards, folgen den sogenannten NIST-Empfehlungen (AES128) und haben keine bekannten Schwachstellen. Wir sichern zu, dass wir die Algorithmen ordnungsgemäß einsetzen. Ein Algorithmus alleine ist keine Garantie für Sicherheit. Wichtig ist es, die Entwicklung zu verfolgen und in der Lage zu sein, den Algorithmus zu verändern[1].

- Wir haben keine eigenen Algorithmen entwickelt, sondern die bestmögliche Kombination an Sicherheitselementen implementiert, um Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Befehlen zu gewährleisten.

- Mit OMNIA 3.0 ist ein mehrschichtiges Sicherheitssystem möglich, in dem die Verschlüsselung im Kommunikationsnetz mit End-to-end-Sicherheit kombiniert wird. So erfolgt jegliche Kommunikation zwischen Head-end-System und Zähler auf sicherem Wege. Hacker haben keine Möglichkeit, sich dazwischenzuschalten und beispielsweise zuvor gesandte Befehle erneut zu senden.

- Alle Komponenten eines OMINA-Systems schützen sich gegenseitig und sich selbst über einen sogenannten rollenbasierten Zugang. In der Praxis bedeutet dies, dass ein Systemnutzer nur jene Zugriffsrechte hat, die seiner Benutzerrolle entsprechen. Dies gilt für die komplette Übertragungskette, vom Zähler bis zu den Servern im Rechenzentrum.

- Informationen zu Verbrauchsdaten und dem physischen Standort des Zählers werden zu keinem Zeitpunkt gemeinsam übermittelt.

- Wir überwachen genau, was auf der Sicherheitsseite geschieht, und stellen sicher, dass unsere Zähler und AMI-Systeme stets die neuesten und besten Verschlüsselungsalgorithmen verwenden.

- Unser gesamter Entwicklungsprozess unterliegt besonderen Richtlinien, die sicherstellen, dass die erforderlichen Sicherheitselemente im Endprodukt wirksam sind. Bei der Sicherheit gehen wir keine Kompromisse ein und prüfen alle Einzelheiten der gegebenen Anforderungen, der Sicherheitsverschlüsselung und der durchgeführten Tests. Hierbei ist vor allem die Zertifizierung nach ISO 27001 hervorzuheben.

- Das OMNIA-System von Kamstrup wurde gemäß den gestaffelten Sicherheitsgrundsätzen konzipiert. Das bedeutet, wenn irgendeine Einheit im Netzwerk gehackt werden sollte, wird der potenzielle Schaden eingegrenzt. So kann ein gehackter Stromzähler zum Beispiel weder das System noch andere Zähler beeinflussen.

[1] Ein Algorithmus ist eine Berechnungsmethode, eine Art Formel, die in diesem Fall zusammen mit dem Kodierungsschlüssel dazu verwendet wird, lesbare Daten in verschlüsselte Daten zu verwandeln.

Wer prüft, ob die Sicherheit gewährleistet ist?

Kamstrup nimmt Datensicherheit sehr ernst. Daher wird die Datensicherheit in Produkten und Systemen von Kamstrup regelmäßig durch externe Experten renommierter Sicherheitsunternehmen[2] überprüft.

Erfüllt der Stromzähler die allgemeinen Standards für Datensicherheit?

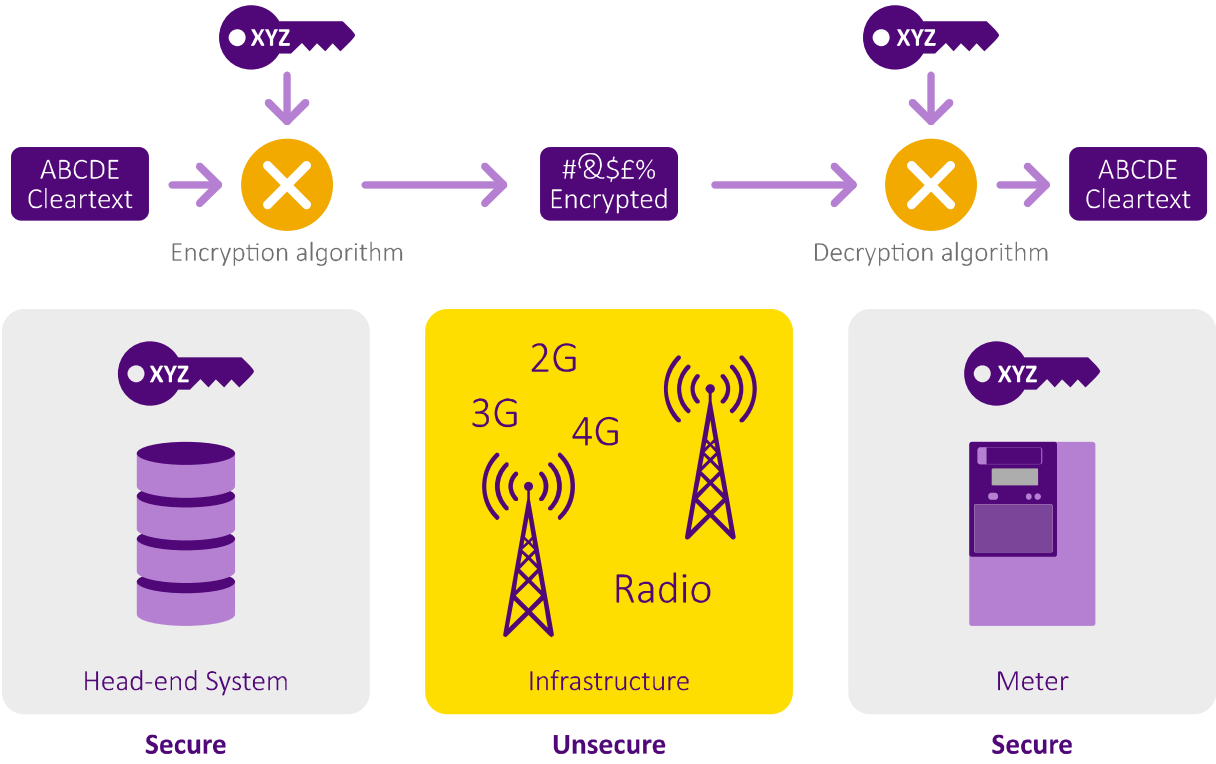
Ja. Der OMNIPOWER-Zähler erfüllt die für alle Stromzähler geltenden Richtlinien zur Datensicherheit und darüber hinaus die einschlägigen Datensicherheitsstandards für das Internet. Beispiele hierfür sind VPN-Tunnel[3], Verschlüsselung mit dem AES128-CCM-Algorithmus und die Verwendung eindeutiger Kodierungsschlüssel für jeden Stromzähler. Zusammen gewährleisten diese Mechanismen die Datensicherheit. Eine wesentliche Voraussetzung hierfür ist, dass die OMNIPOWER-Zähler so konstruiert sind, dass sie nur jene Kommunikation zulassen, die mit dem richtigen Kodierungsschlüssel verschlüsselt wurde. Ohne den korrekten Kodierungsschlüssel kann nicht einmal ein Wartungstechniker des Versorgungsunternehmens oder von Kamstrup selbst mit dem Stromzähler kommunizieren.

[2] CSIS und Alexandra Institute

[3] Virtual Private Network (VPN) ist eine beliebte Methode zur Herstellung und Aufrechterhaltung einer sicheren Verbindung zwischen den Einheiten in einem unsicheren Netzwerk, wie etwa dem Internet.

Was ist ein Kodierungsschlüssel?

Ein Kodierungsschlüssel tut in etwa das gleiche wie Ihr Haustürschlüssel. Ohne den richtigen Schlüssel bekommen Sie die Tür nicht auf und können Ihr Haus nicht betreten. Genauso kann eine verschlüsselte Nachricht nicht entschlüsselt (geöffnet) werden, wenn der passende Kodierungsschlüssel fehlt. Dies wird über den Verschlüsselungsalgorithmus sichergestellt.



Können andere sehen, wieviel ich verbrauche?

Normalerweise nicht. Gemäß geltenden Gesetzen müssen Verbraucher die Möglichkeit haben, ihre Stromrechnung mit dem Stromverbrauch abzugleichen. Der Stromzähler entspricht den geltenden Gesetzen und die Verbraucher können sich jederzeit Verlaufsdaten zum Verbrauch auf dem Zählerdisplay ansehen. Die gleichen Verbrauchsmessungen können auch auf einem drahtlosen Anzeigegerät dargestellt werden, das mit dem Stromzähler verbunden ist. Die Verbindung zwischen dem Stromzähler und dem Anzeigegerät ist verschlüsselt, sodass nur das Anzeigegerät des Verbrauchers den Stromverbrauch darstellen kann.

Wird der Stromzähler vom Versorgungsunternehmen ausgelesen, geschieht dies auf einem Kommunikationsweg, der über mehrere Datensicherheits-Mechanismen, inklusive Verschlüsselung, gesichert ist. Diese Mechanismen schützen die Kommunikation wirksam vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit. In der Praxis bedeutet dies, dass die Nachrichten, die zwischen dem Stromzähler und dem Versorgungsunternehmen übermittelt werden, weder abgehört, verändert, kopiert noch wiederverwendet werden oder verschwinden können.

Verbrauchsdaten werden in sicheren Datenbanken gespeichert, die nur denjenigen Mitarbeitern des Versorgungsunternehmens (oder von Kamstrup) zugänglich sind, die berechtigterweise auf diese Daten zugreifen müssen. Dabei kann es sich auch um einen Kundendienstmitarbeiter handeln, der in Kontakt mit einem Verbraucher steht.

Kann ein Verbraucher in einer Mietwohnung den vorherigen Verbrauch einsehen?

Die fernauslesbaren Stromzähler speichern die Verbrauchswerte mindestens 6 Monate lang, sodass die Stromrechnung mit den Verbrauchsdaten der Zähleranzeige verglichen werden kann.

Wie kann ich mich vergewissern, dass der Stromzähler korrekt misst?

Der OMNIPOWER-Zähler ist in der EU gemäß der Messgeräterichtlinie (MID) typgeprüft. Die MID ist ein gemeinsames europäisches Kennzeichnungssystem, das die nationalen Zulassungen im Jahr 2006 ersetzte. Die MID gilt für alle Verbrauchszähler, einschließlich der Stromzähler von Kamstrup. Mit einer MID-Typenzulassung können Zählerdaten direkt für die Abrechnung des Stromverbrauchs verwendet werden.

Der Test, nach dem eine Typenzulassung erteilt wird, wird von einer sogenannten Prüfstelle durchgeführt. Die Stromzähler von Kamstrup werden bei NMI in den Niederlanden geprüft. Beim Typentest werden alle Kommunikationsmodule zusammen mit dem Zähler getestet, um sicherzustellen, dass die gesetzlichen Messungen (Energiemessungen usw.) und Berechnungen nicht unterbrochen oder beeinträchtigt werden.

Das bedeutet, dass Stromzähler von Kamstrup, die Funkmodule enthalten, zertifiziert und zugelassen sind. Ihre Verwendung ist daher in der EU und in Ländern, die die Konformität mit der EU-Gesetzgebung anerkennen, zum Beispiel Norwegen, legal.

Wie kann ich mich vergewissern, dass sich niemand in meinen Stromzähler gehackt hat?

Der OMNIPOWER-Zähler ist so konzipiert und gebaut, dass er vor jeglichen Eindringversuchen, sowohl physischer Art (was in der Regel sichtbare Spuren am Zähler hinterlässt) als auch in Form von Hackerangriffen, sicher ist
Jeder Versuch, den Zähler zu hacken, wird von diesem erfasst und automatisch an das Versorgungsunternehmen gemeldet. Dadurch ist das Versorgungsunternehmen in der Lage, einen Techniker vor Ort zu schicken, um das Problem zu begutachten.

Auch alle elektronischen Aktivitäten im Zähler werden überwacht, um Hackerangriffe zu verhindern. Die Kommunikation mit dem Zähler ist vollständig verschlüsselt, was den Zähler und die Daten vor Hackerangriffen schützt. Gleichzeitig verfügt der Zähler über einen Schutzmechanismus, der sicherstellt, dass nur Kommunikation vom Versorgungsunternehmen angenommen wird. Die Kommunikation mit dem Zähler kann auch durch das Versorgungsunternehmen überwacht werden, sodass jegliche unerwünschte Kommunikation mit dem Zähler erkannt werden kann.

Kann der Zähler manipuliert werden?

Die fernauslesbaren Stromzähler sind für die korrekte Erfassung des Verbrauchs konstruiert und nicht für externe Faktoren wie starke magnetische Felder oder physische Einwirkungen anfällig. Dennoch bewirken beide Arten der Manipulation, dass der Stromzähler einen Alarm an das Versorgungsunternehmen sendet.

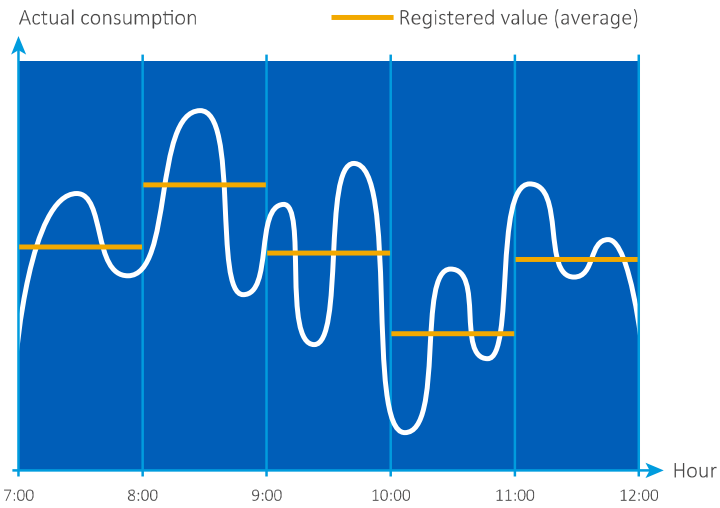
Was wird bei einem fernauslesbaren Stromzähler gemessen?
Die OMNIPOWER-Zähler von Kamstrup sind für Abrechnungszwecke zugelassen. Die Stromzähler erfassen also regelmäßig den Stromverbrauch und senden den gemessenen Verbrauch an das Versorgungsunternehmen.

In der Praxis wird der Stromverbrauch über einen bestimmten Zeitraum zusammengefasst und am Ende jedes Zeitraums registriert. Die Dauer dieser Zeiträume wird vom Versorgungsunternehmen definiert, wobei der OMNIPOWER-Zähler keine kürzere Periode als 15 Minuten zulässt (Perioden von 15, 30 und 60 Minuten sind wählbar). Das bedeutet, dass der in gewählten Zeitperiode anfallende Stromverbrauch addiert und dem Versorgungsunternehmen als ein Wert präsentiert wird. Anhand dieser Werte ist es dem Versorgungsunternehmen nicht möglich, festzustellen, wofür Sie den Strom verwendet haben oder wann genau der Verbrauch stattgefunden hat. Die meisten Versorgungsunternehmen nutzen 60-Minuten-Intervalle, da dies den gesetzlichen Anforderungen entspricht.

Für welche Zwecke können die Daten verwendet werden?
Die Daten werden für zweierlei Zwecke erfasst. Einerseits werden diese für die Rechnungslegung verwendet, andererseits können damit die Qualität sichergestellt und das Stromnetz optimiert werden.

Dem Versorgungsunternehmen stehen verschiedene Messgrößen zur Verfügung, die Aufschluss über die Qualität des Stroms liefern. Unter anderem können die OMNIPOWER-Zähler verschiedene Arten von Stromunterbrechungen und Spannungsabfällen, Spannungsschwankungen, Phasenverschiebungen sowie den Klirrfaktor (THD) erfassen. Diese Parameter werden vom Versorgungsunternehmen genutzt, um festzustellen, ob die Qualität des Stroms ausreichend ist.

Die gesammelten Daten können nicht für die detaillierte Analyse des Verbraucherverhaltens genutzt werden, da diese nur Durchschnittswerte der 15-, 30- oder 60-Minuten Ausleseperiode darstellen. Die unten angeführte Grafik veranschaulicht das.



(comment: Actual consumption = aktueller Verbrauch
Registered value (average) = Registrierter Durchschnittswert

Werden die Daten bereits im Zähler verschlüsselt?

Die Daten werden verschlüsselt, sobald sie den Verbrauchszähler verlassen. Im Zähler selbst sind die Daten nicht verschlüsselt.
Die Daten können per Direktzugriff auf den Zähler ausgelesen werden. Dies kann entweder über das Zählerdisplay oder ein sogenanntes optisches Auge, ein Auslesegerät (Kabelverbindung), erfolgen. Hierzu muss allerdings physischer Zugang zum Zähler sowie zum passenden Kodierungsschlüssel bestehen, da nur so, die über das optische Auge ausgelesenen Daten, entschlüsselt werden können.

Welcher Verschlüsselungsstandard kommt zum Einsatz?

Die Stromzähler können nur mit dem richtigen Kodierungsschlüssel ausgelesen werden, der jeweils nur für einen einzelnen Stromzähler gültig ist. Nichtverschlüsselte Anfragen an den Stromzähler werden somit vom Zähler nicht beantwortet. Die Daten werden verschlüsselt, sobald sie den Zähler verlassen, ganz egal ob sie über das Funknetzwerk, eine Punkt-zu-Punkt-Verbindung oder das optische Auge versandt werden.

In jedem Fall kommt eine Verschlüsselung auf zwei Ebenen zum Einsatz, bei der zwei verschiedene, einmalige Kodierungsschlüssel benötigt werden, um Daten abzufragen und die Antwort zu entschlüsseln. Beide Verschlüsselungsebenen verwenden den AES128-Bit-Verschlüsselungsalgorithmus, der in der Sonderveröffentlichung des NIST mit der Bezeichnung 800-38C beschrieben ist.

Hält sich Kamstrup an das Datenschutzgesetz?

Die fernauslesbaren Zähler erfassen Daten, die gemäß den Bestimmungen des Datenschutzgesetzes geschützt werden müssen. Diese Bestimmungen werden vollumfänglich erfüllt. Die erfassten Daten werden keinem Dritten verfügbar gemacht, sofern betriebliche oder geschäftliche Zwänge dies nicht erfordern. Beispielsweise können die Kundendienstmitarbeiter auf die Verbrauchsdaten zugreifen, wenn ein Verbraucher anruft und diesbezügliche Fragen stellt.