Vom Zähler in die Cloud

Die sichere und einfache Erfassung von Verbrauchsdaten mittels AWS IoT Core

Vorstand, Dr. Jürgen Nützel

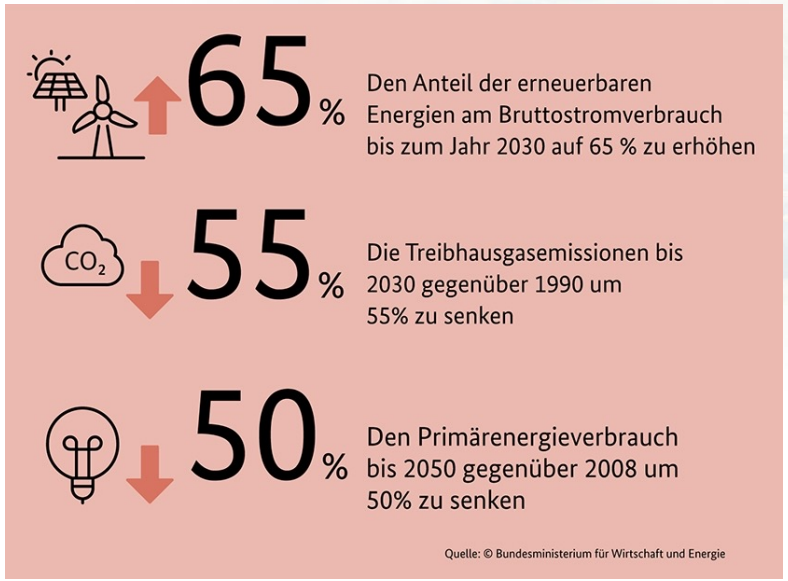
4FriendsOnly.com
Internet Technologies AG

4FriendsOnly.com Internet Technologies AG

- Spin-off von Fraunhofer IDMT & TU Ilmenau
- CEO, Privatdozent und Haupteigner: Dr. Jürgen Nützel
- E-Commerce Experten (> 10 Jahre)
- Intershop Partner (seit fast 10 Jahren)
- Cloud Computing (AWS seit 2013)
- Amazon AWS Partner seit 2017
- Mit dem Umzug in ein größeres Büro in Ilmenau wurde der Wachstumsplan gestartet
- 20 Mitarbeiter in Ilmenau aus 6 Nationen plus
- 3 Mitarbeiter in Indien (im Bundesstaat Gujarat)

Oberbürgermeister Dr. Daniel Schultheiß zu Besuch im Juni

Ziele der Energiewende und …



… ihre Umsetzung bringen einige neue Forderung mit sich:

- Kunden müssen aktuelle Verbrauchswerte einsehen können.
- Zeitabhängige Tarife sollen möglich werden.
- Bei Strom ist auch die Steuerbarkeit zur Stabilisierung der Netze notwendig.

Daher muss der Rollout intelligenter Messsysteme (Smart Metering) erfolgen.

Smart Metering – Was ist das?

„Smart Metering ist das computergestützte Messen, Ermitteln und Steuern von Energieverbrauch und -zufuhr.

…

Smart Meter sind intelligente, vernetzte Zähler für Ressourcen und Energien wie Wasser, Gas oder Strom. …“

Quelle:
https://wirtschaftslexikon.gabler.de/definition/smart-metering-53998

Smart Metering – Einige Vorteile

Echtzeit-daten

Smart Meter ermöglichen den Nutzern, ihren Energieverbrauch in Echtzeit zu verfolgen. Dies soll dazu beitragen das Bewusstsein für den eigenen Verbrauch zu erhöhen.

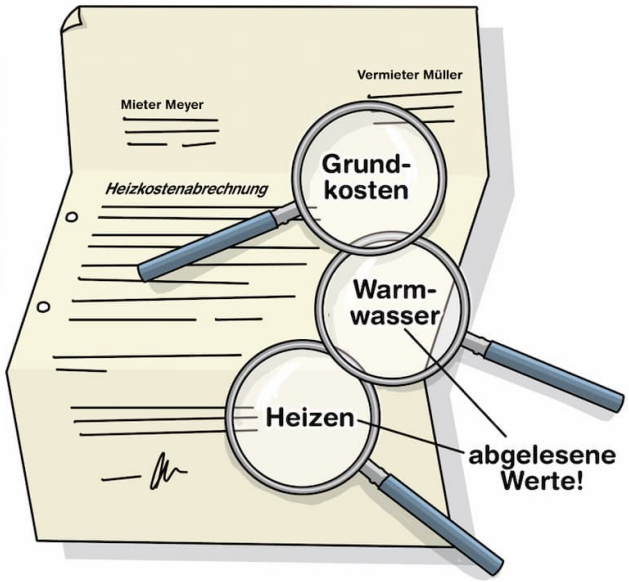
Kosten-ersparnis

Durch das Verständnis und die Anpassung des Verbrauchsverhaltens können Nutzer Energie sparen und dadurch Kosten reduzieren. Bei Strom können auch zeitabhängige Tarife dazu beitragen. Daneben gibt es Potentiale Last in andere Zeiten zu verschieben.

Digitalisierung des Ablesens

Mit Smart Metern ist keine manuelle Ablesung mehr erforderlich, was den Aufwand für den Vermieter reduziert.

Am Beispiel – Heizkostenabrechnung



Es gibt nicht nur Stromzähler. Es gibt Heizkostenverteiler. Zum Beispiel bei einem Mietobjektes mit mehreren Parteien, welches eine zentrale Heizung bzw. Warmwasserversorgung besitzt.

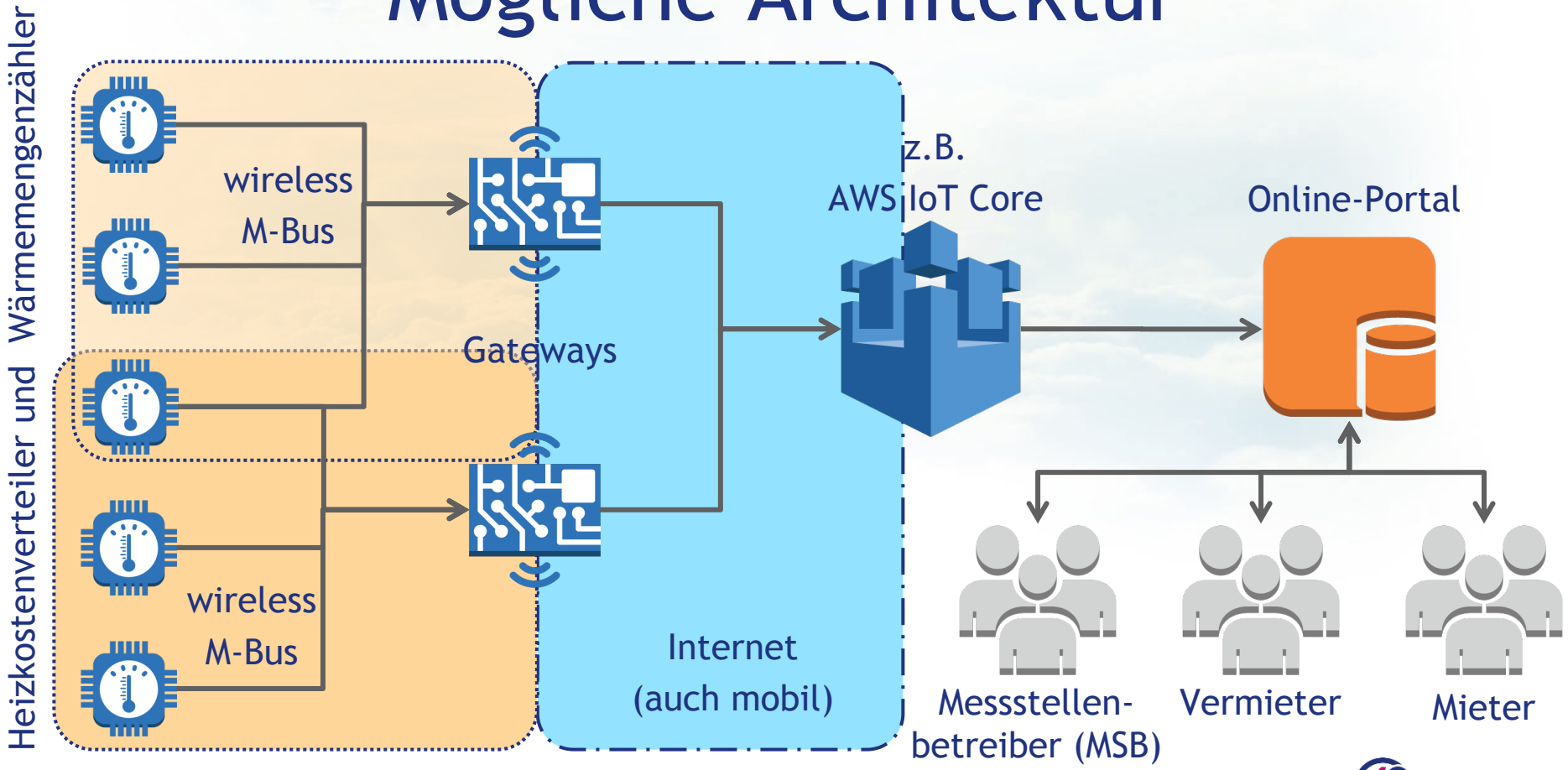
Rechtliche Basis bildet die Heizkostenverordnung, die einige Neuerungen zu Smart-Metering bietet:

- Monatliche Verbrauchsinfo ab 1.1.2022
- Kürzungsrecht (15%) für nicht verbrauchsabhängige Abrechnung

Quelle: https://www.gesetze-im-internet.de/heizkostenv/

Bild Quelle: https://www.heizsparer.de/spartipps/heiznebenkosten/heizkostenabrechnung

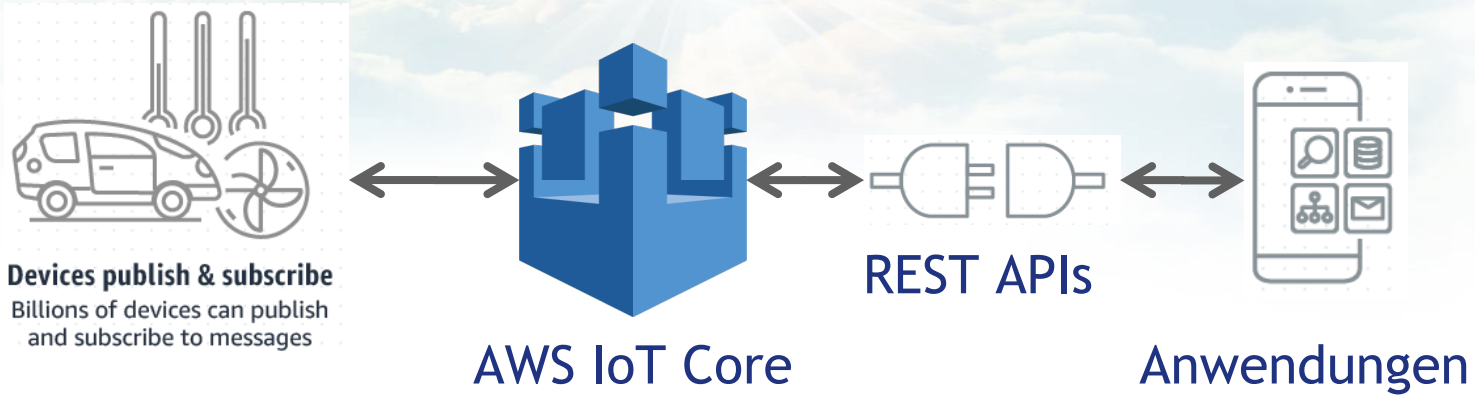
Mögliche Architektur



Was ist AWS IoT Core?

Mit AWS IoT Core kann man Milliarden von IoT-Geräten verbinden und Billionen von Nachrichten an AWS-Services weiterleiten, ohne die Infrastruktur zu verwalten.

Außerdem lassen sich Anwendungen erstellen, mit deren Hilfe die Benutzer diese **Geräte über ihre Smartphones oder Tablets steuern** können.



Quelle: https://docs.aws.amazon.com/de_de/iot/latest/developerguide/what-is-aws-iot.html

Wichtige Komponenten AWS IoT Core

Message Broker: Später mehr dazu

Rules Engine:
Kann selektierte Nachrichten(-Teile) an Cloud-Endpunkte wie AWS Lambda-Funktionen, AWS S3 (Cloud Speicher) oder in eine TimestreamDB weiterleiten.

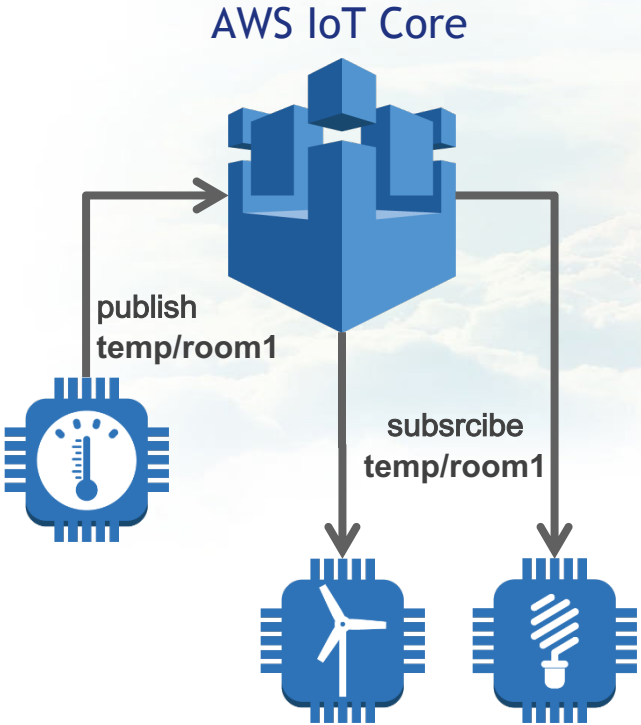
Registrierung (Registry):
Organisiert die Ressourcen, die jedem Gerät in der AWS Cloud zugeordnet sind. Um Geräte besser verwalten und Fehler beheben zu können, können Sie jedem Gerät Zertifikate (später mehr) und MQTT-Client-IDs zuordnen.

Device Shadow-Service und **Geräteschatten**: Später mehr dazu

Device Gateway:
Ermöglicht Geräten die sichere und effiziente Kommunikation mit AWS IoT.

Quelle: https://docs.aws.amazon.com/de_de/iot/latest/developerguide/what-is-aws-iot.html

Message-Broker

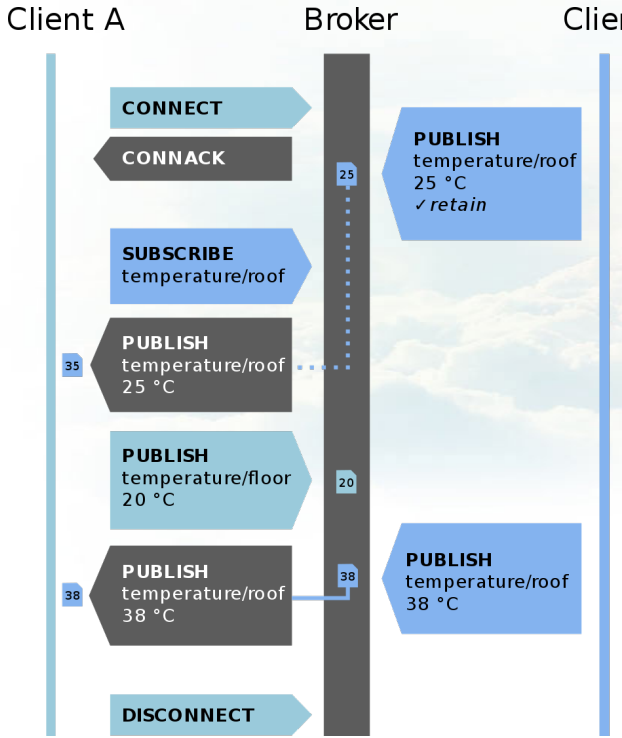


... ist ein Broker-Dienst zur Veröffentlichung und dem Abonnement von Status-Nachrichten. Bei der Kommunikation mit AWS IoT Core sendet ein Gerät eine Nachricht an ein Topic (z.B. Sensor/temp/room1). Der Message Broker sendet darauf die Nachricht an alle Geräte, die dieses Topic abonniert haben.

Das Versenden der Nachricht bezeichnet man als *Veröffentlichen (publishing)*. Sich für den Empfang von Nachrichten zu einem bestimmten Topic zu registrieren, bezeichnen man als *Abonnieren (subscribing)*.

Quelle: https://docs.aws.amazon.com/de_de/iot/latest/developerguide/iot-message-broker.html

Protokolle und MQTT

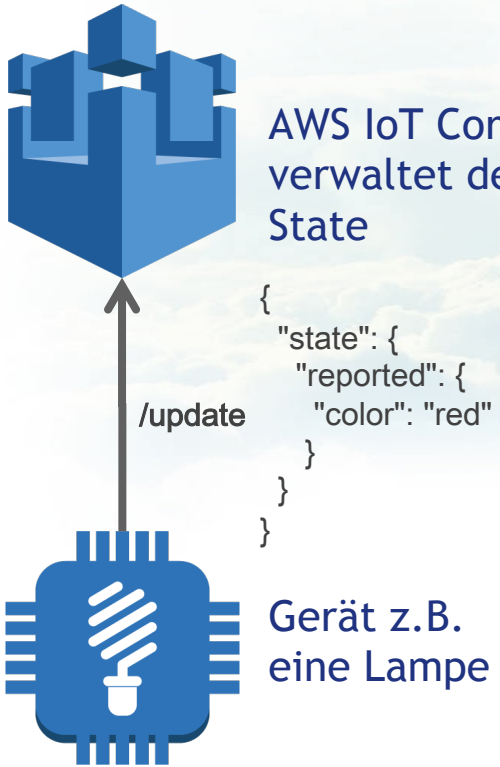


Der Message-Broker nutzt das MQTT-Protokoll. MQTT wird zusätzlich auch über das WebSocket-Protokoll unterstützt. Bei einer HTTP-Verbindung erfordert jede Aktion des Servers eine vorhergehende Anfrage des Clients.

Beim WebSocket-Protokoll bleibt die Verbindung geöffnet. Der Server (Broker) kann dann diese offene Verbindung neue Informationen an den Client ausliefern, ohne auf eine neue Verbindung des Clients zu warten.

Quellen: https://docs.aws.amazon.com/de_de/iot/latest/developerguide/protocols.html, https://de.wikipedia.org/wiki/MQTT
Abbildung von Simon A. Eugster - Eigenes Werk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=70622928

Device Shadow-Service



Der Device Shadow-Services verwendet reservierte MQTT-**Topics**, um es Anwendungen und Geräten zu ermöglichen, die Statusinformationen für ein Gerät (Schattengerät) abzurufen, zu aktualisieren oder zu löschen.

Die Namen dieser Topics beginnen mit $aws/things/*thingName*/shadow.

Die Lampe aktualisiert hiermit ihren Schatten: $aws/things/myLightBulb/shadow/update

Quelle: https://docs.aws.amazon.com/de_de/iot/latest/developerguide/device-shadow-data-flow.html

Verbrauchsdaten sind

vertraulich **und** privat

Daher müssen wir auf die Sicherheit (Security) schauen…

Schutzziele der Informationssicherheit

Vertraulichkeit

Daten dürfen lediglich von autorisierten Benutzern gelesen werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.

Integrität

Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.

Verfügbarkeit

Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

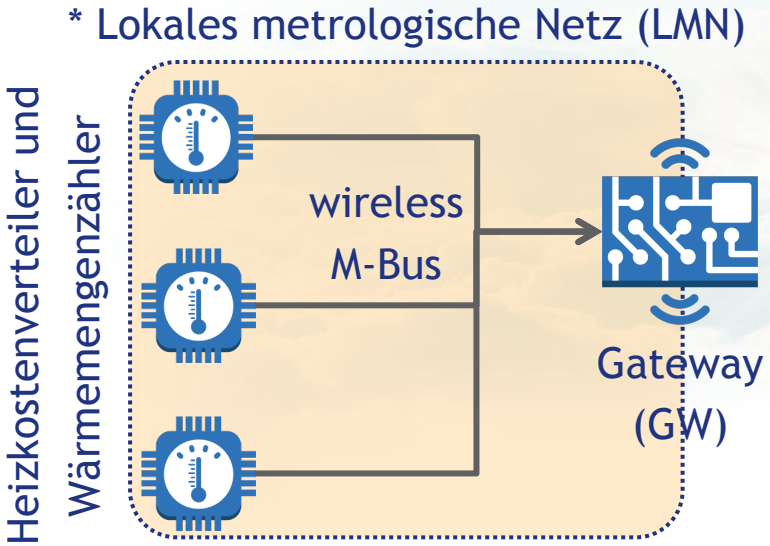
Quelle: https://de.wikipedia.org/wiki/Informationssicherheit

Weiteres übergeordnetes Ziel

Authentizität

Unter Authentizität versteht man sowohl einen Identitätsnachweis als auch die Authentizität der eigentlichen Daten. Es gilt zu gewährleisten, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.

Die Messwerte müssen …



… verschlüsselt per Funk (wireless M-Bus) an das Gateway (GW) übertragen werden.

Jeder Sensor nutzt seinen eigenen/individuellen 128-Bit AES Schlüssel.

* Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html

Das Gateway sollte …

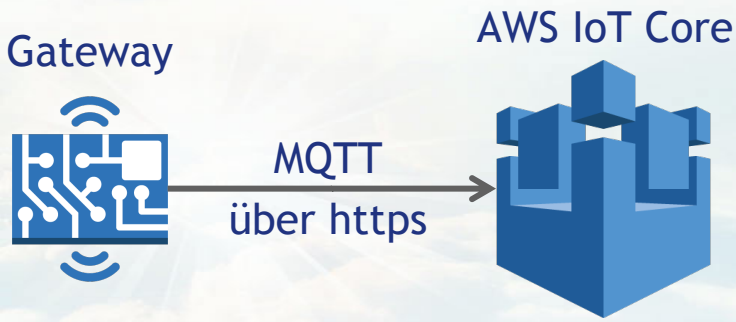


Bild Quelle: https://www.solvimus.de/en/product/muc-one-2/

… die Messwerte mehrerer Sensoren in seiner Nähe gebündelt in die Cloud übertragen. Die Heizkostenverteiler sind über den wireless M-Bus (LMN) an das Gateway angebunden. Das GW (z.B. MUC.one mit eigener SIM) überträgt die gebündelten Messdaten in die Cloud. Es übernimmt die Autorisierung gegenüber AWS IoT Core. Es werden dazu Zertifikate genutzt …

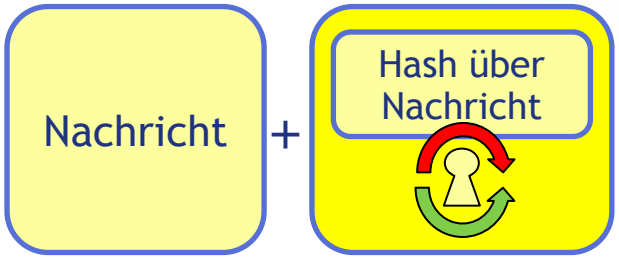
Einschub: Public-Key-Kryptographie

- Grundprinzip (ganz kurz)
  - Es gibt zwei Schlüssel (=Schlüsselpaar)
  - Was mit dem einen verschlüsselt wird kann nur mit dem anderen entschlüsselt werden (=asymmetrisch)
  - Der eine Schlüssel heißt öffentlich: Public Key
  - Der andere Schlüssel heißt privat: Private Key

Asymmetrische Verschlüsselung

Nachricht mit Public Key des Empfängers verschlüsselt

Digitale Signatur

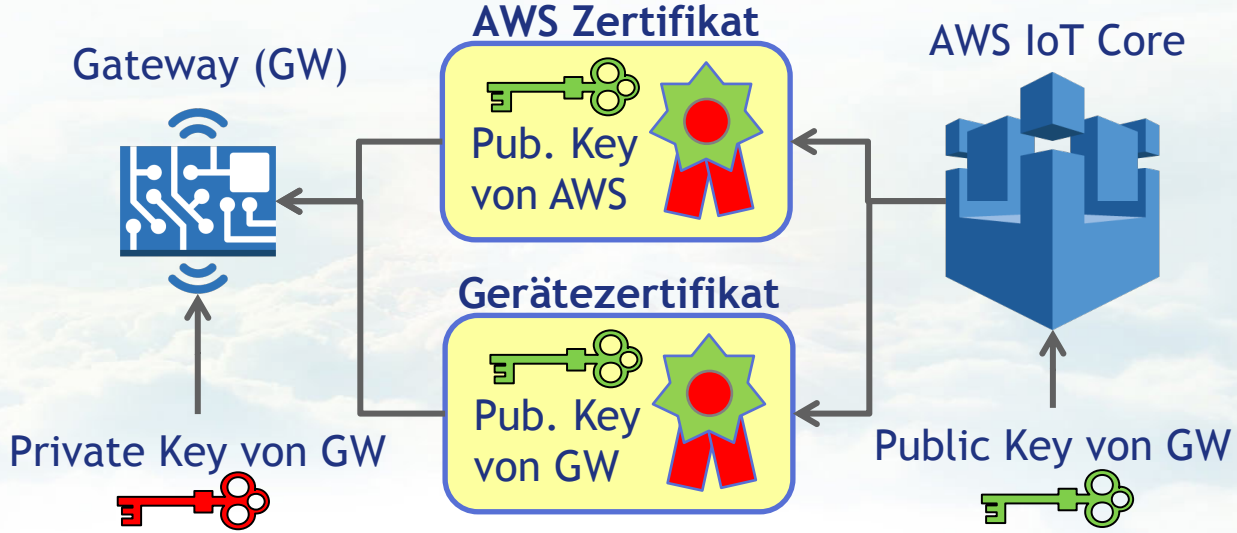


Hash über Nachricht mit Private Key des Senders verschlüsselt

Zertifikate

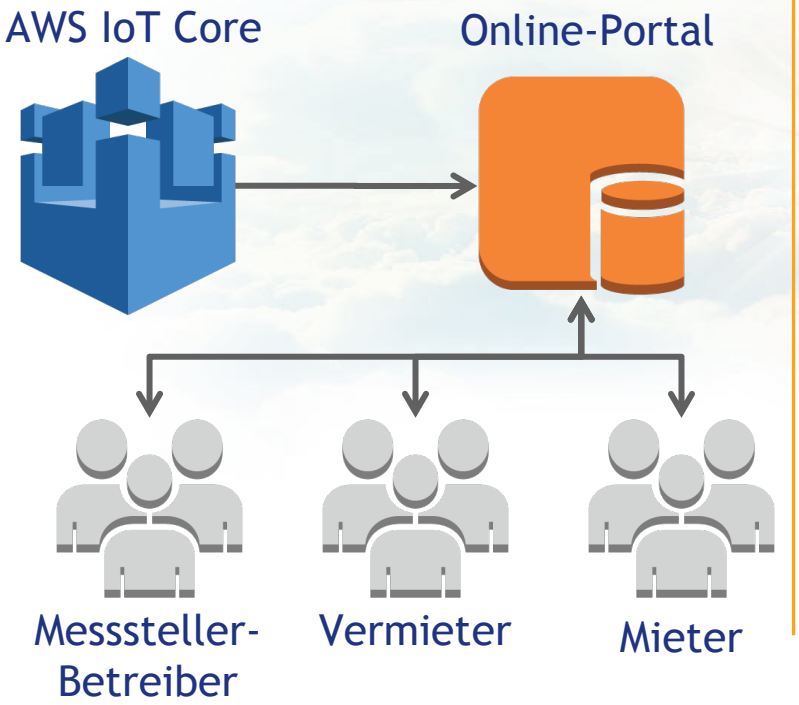
- Öffentliche Schlüssel werden ausgetauscht
  - Dem öffentliche Schlüssel alleine darf man noch nicht trauen
  - Er muss von einer dritten Instanz (CA – Certification Authority) signiert („beglaubigt“) werden
- Das Ergebnis nennt sich Zertifikat:
  - Enthält den öffentliche Schlüssel und
  - Einen Datensatz über den Besitzer des Schlüssel
  - Beides zusammen wurde von der CA digital signiert
  - AWS hat in diesem Fall die Rolle der CA

Beim Setup des Gateways …



… werden in Fertigung mittels einer PKI (Public-Key-Infrastructure) Schlüsselpaare erstellt. Der öffentliche Schlüssel wird von AWS signiert. D.h. AWS erstellt davon ein spezifisches Gerätezertifikat. Daneben wird das AWS Zertifikat und der private Key in das Gateway einprogrammiert. Der private Key sollte danach in der Fertigung gelöscht werden.

Das Online-Portal …



… zur Heizkostenabrechnung greift auf die Messwertdaten im AWS IoT Core zu.

Es ermöglicht Vermietern verbrauchsabhängige Abrechnungen zur erstellen.

Es bietet Mietern eine transparente Darstellung ihrer Verbrauchsdaten in nahezu Echtzeit.

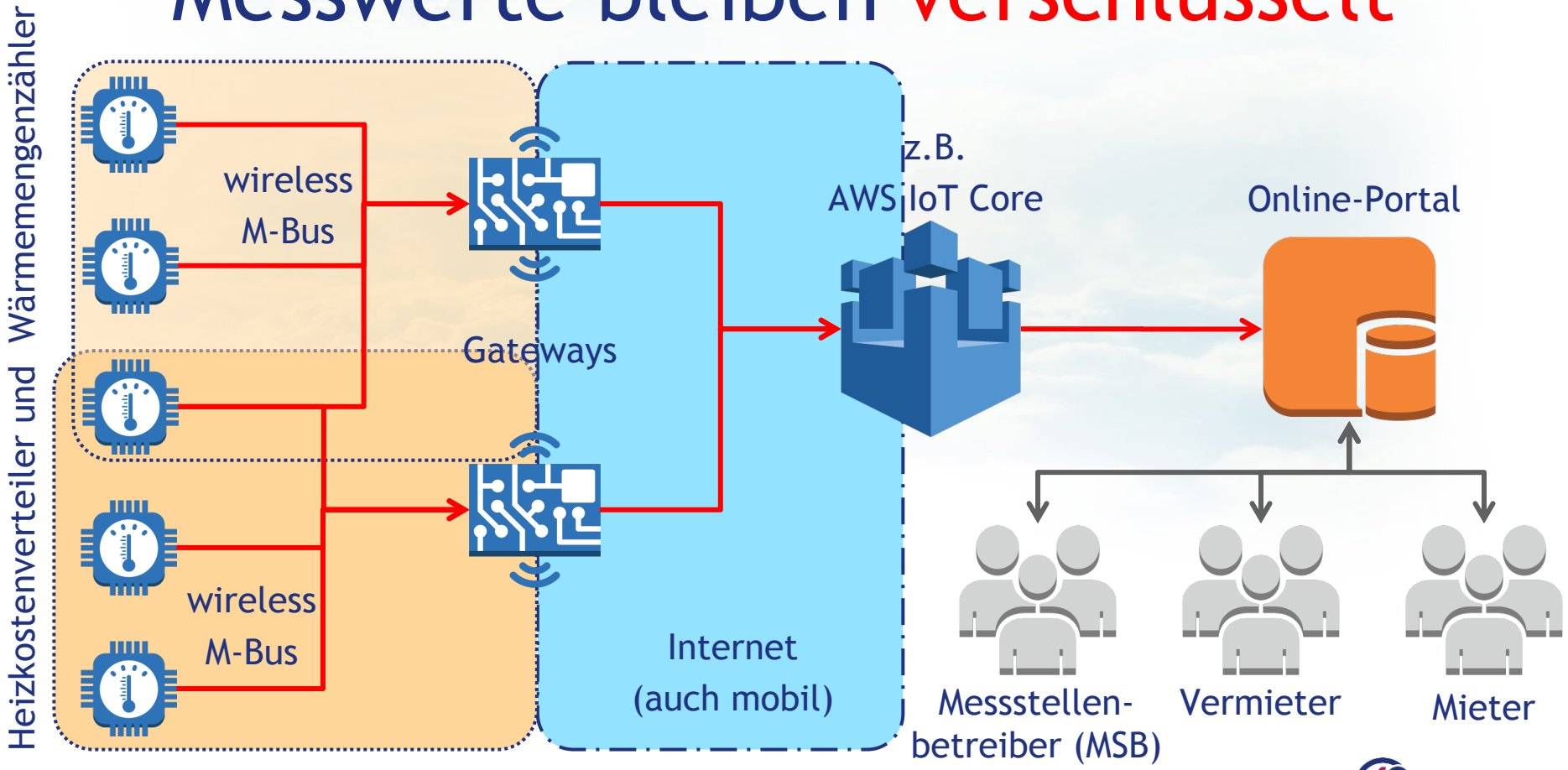
Vermieter sehen Verbrauchsdaten ihrer Mieter nur aufsummiert (Privatheit!)

Messstellenbetreiber verwalten hierrüber Heizkostenverteiler und Gateways.

Was machen wir anders

- Kein Smart Meter Gateway
- Messwerte werden nicht im Gateway entschlüsselt
- Nur das Online-Portal kennt die Schlüssel der Heizkostenverteiler
  - Dadurch leichter Setup der Gateways
  - AWS IoT Core hat keinen Zugriff auf private Daten!
- Trennung AWS IoT Core und Online-Portal

Messwerte bleiben verschlüsselt



Diskussion einiger Angriffsszenarien

- Mithören des M-Bus Funkkanals
  - Möglich aber wirkungslos
- Replay von Zählerständen
  - Nicht möglich. Counter sorgt für individuelle Telegramme
- DoS, Funkkanal überlasten
  - Möglich aber Schaden überschaubar
- Zähler manipulieren
  - Zähler haben eine Tamper-Detection
- Gateway klonen durch Auslesen des private Keys
  - Wirkungslos, wenn man die Zähler nicht auch klont
- Man-in-the-Middle (zwischen Gateway und AWS)
  - Wird durch Zertifikate verhindert
- Zählerschlüssel werden aus Portal gestohlen
  - Theoretisch nicht wirklich verhinderbar. Geschützt durch übliche Sicherheitsmaßnahmen

Ankündigung

- Partnerschaft 4FO und solvimus
  - 4FO entwickelt und betreibt für solvimus einen Online-Service
  - solvimus bringt den Online-Service unter seinen Namen an den Markt

Ausblick

- Internationalisierung
- Wasserversorgung
  - ist in vielen Regionen der Welt kostbar
- Monitoring-System
  - Durch 15min Messintervalle kann ein Wasserrohrbruch schnell detektiert werden

Vielen Dank

Vorstand, Dr. Jürgen Nützel

4FriendsOnly.com
Internet Technologies AG