From the meter to the cloud

The secure and easy collection of consumption data using AWS IoT Core

CEO, Dr. Jürgen Nützel

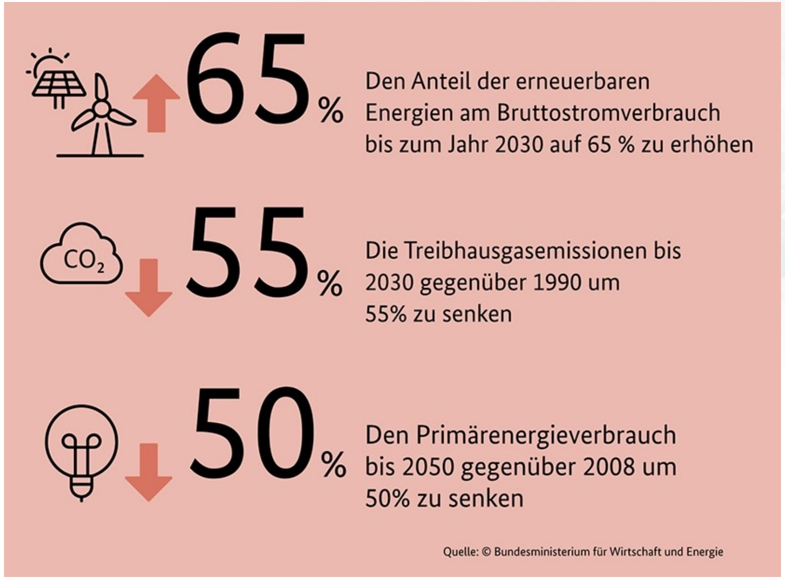
4FriendsOnly.com
Internet Technologies AG

4FriendsOnly.com Internet Technologies AG

- Spin-off of Fraunhofer IDMT & TU Ilmenau
- CEO, Associate Professor and Main Owner: Dr. Jürgen Nützel
- E-Commerce Experts (> 10 years)
- Intershop Partner (for almost 10 years)
- Cloud Computing (AWS since 2013)
- Amazon AWS Partner since 2017
- With the move to a larger office in Ilmenau, the growth plan was started
- 20 employees in Ilmenau from 6 nations plus
- 3 employees in India (in the state of Gujarat)

Lord Mayor
Dr. Daniel Schultheiß
Visiting in June

Goals of the energy transition and…



65 %

Den Anteil der erneuerbaren Energien am Bruttostromverbrauch bis zum Jahr 2030 auf 65 % zu erhöhen

55 %

Die Treibhausgasemissionen bis 2030 gegenüber 1990 um 55% zu senken

50 %

Den Primärenergieverbrauch bis 2050 gegenüber 2008 um 50% zu senken

Quelle: © Bundesministerium für Wirtschaft und Energie

… their implementation entails some new demands:
Customers must be able to view current consumption values.

Time-dependent tariffs are to become possible.

In the case of electricity, controllability is also necessary to stabilize the grids.
Therefore, the rollout of intelligent metering systems (smart metering) must take place.

Smart Metering – What is that?

"Smart metering is the computer-aided measurement, determination and control of energy consumption and supply.

…

Smart meters are intelligent, networked meters for resources and energies such as water, gas or electricity. ..."

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

Smart Metering – Some advantages

Real time-data

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

Cost savings

By understanding and adapting consumption patterns, users can save energy and thereby reduce costs. In the case of electricity, time-dependent tariffs can also contribute to this. In addition, there are potentials to shift load to other times.

Digitization of reading

With smart meters, manual reading is no longer required, which reduces the effort for the landlord.

Using an example – heating cost billing

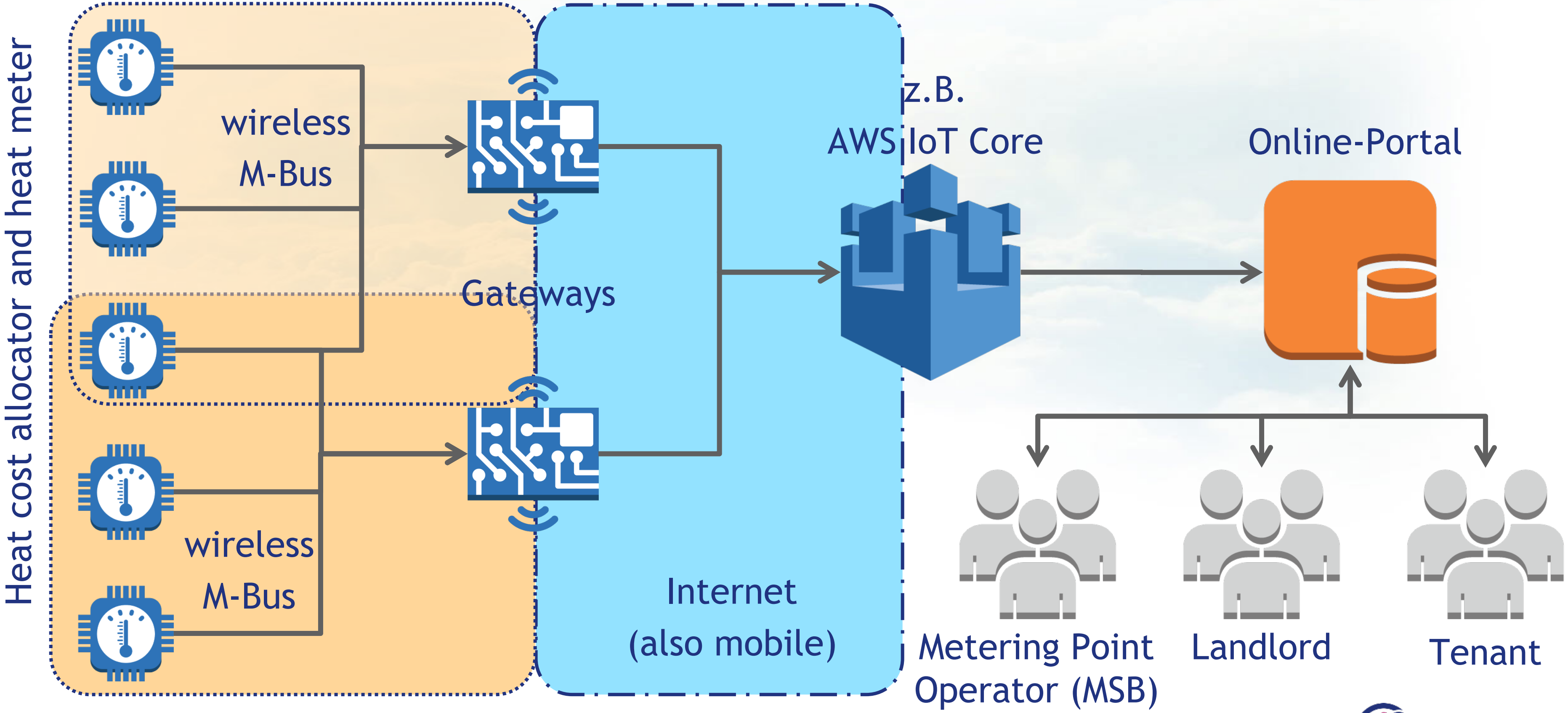
There are not only electricity meters. There are heat cost allocators. For example, in the case of a rental property with several parties, which has a central heating or hot water supply.

The legal basis is the Heating Costs Ordinance, which offers some innovations to smart metering:
Monthly consumption information from 1.1.2022
Right to reduce (15%) for non-consumption-based billing

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

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

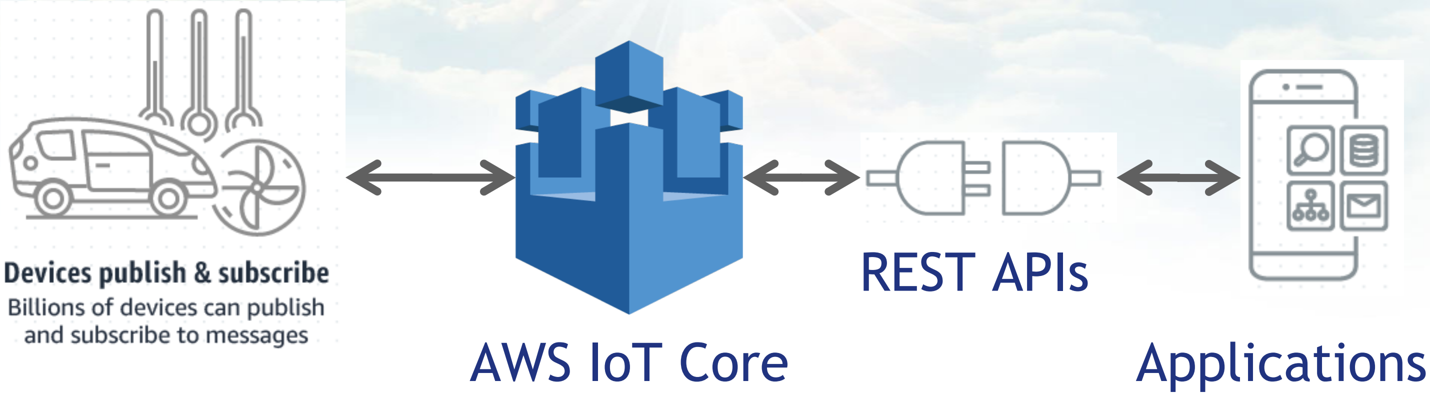
Possible architecture



What is AWS IoT Core?

With AWS IoT Core, you can connect billions of IoT devices and route trillions of messages to AWS services without managing the infrastructure.

It can also create applications that allow users to control these devices from their smartphones or tablets.



Devices publish & subscribe

Billions of devices can publish and subscribe to messages

AWS IoT Core

REST APIs

Applications

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

Key Components AWS IoT Core

Message Broker: More on this later

Rules Engine: Can forward selected messages (parts) to cloud endpoints such as AWS Lambda functions, AWS S3 (cloud storage) or to a TimestreamDB.

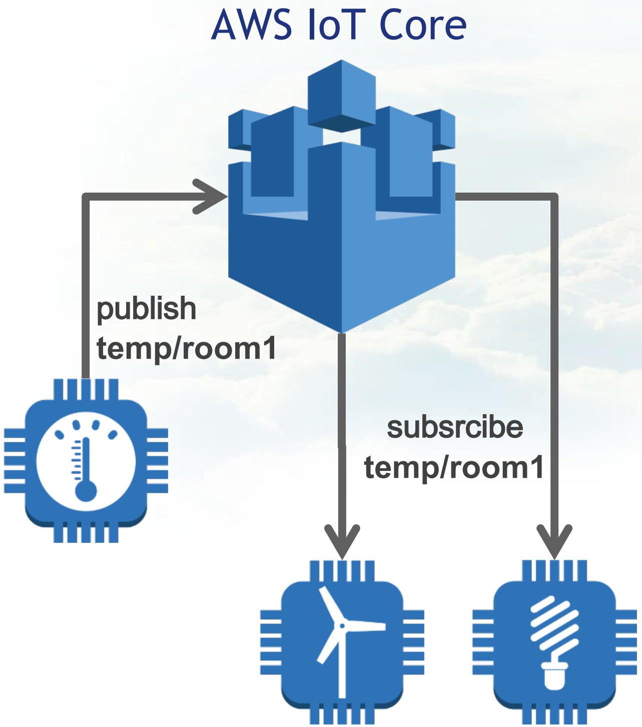
Registry: Organizes the resources associated with each device in the AWS Cloud. To better manage and troubleshoot devices, you can assign certificates (more later) and MQTT client IDs to each device.

Device Shadow Service and Device Shadow: More on that later

Device Gateway: Enables devices to communicate securely and efficiently with AWS IoT.

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

Message Broker

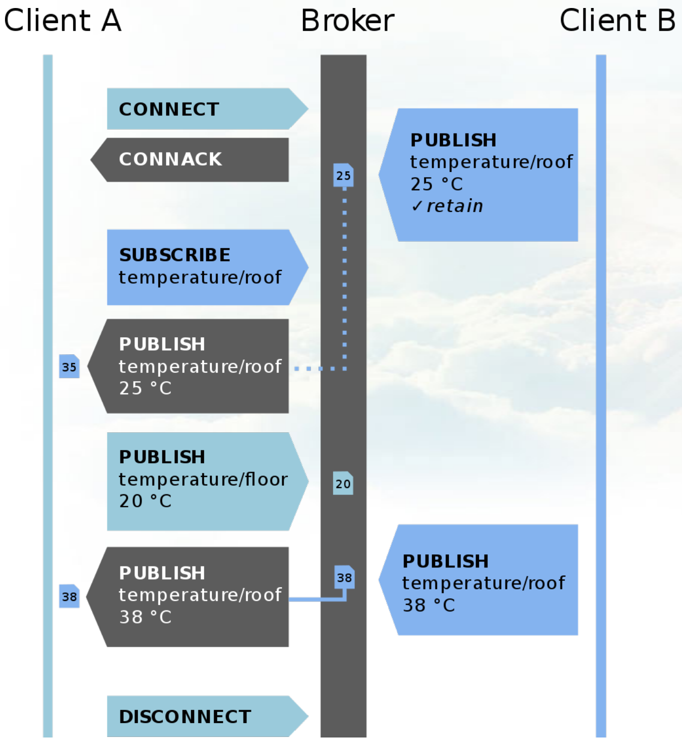


... is a brokerage service for publishing and subscribing to status messages. When communicating with AWS IoT Core, a device sends a message to a topic (for example, Sensor/temp/room1). The message broker then sends the message to all devices that have subscribed to this topic.

The sending of the message is called publishing. Registering to receive messages on a specific topic is called subscribing.

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

Protocols and MQTT



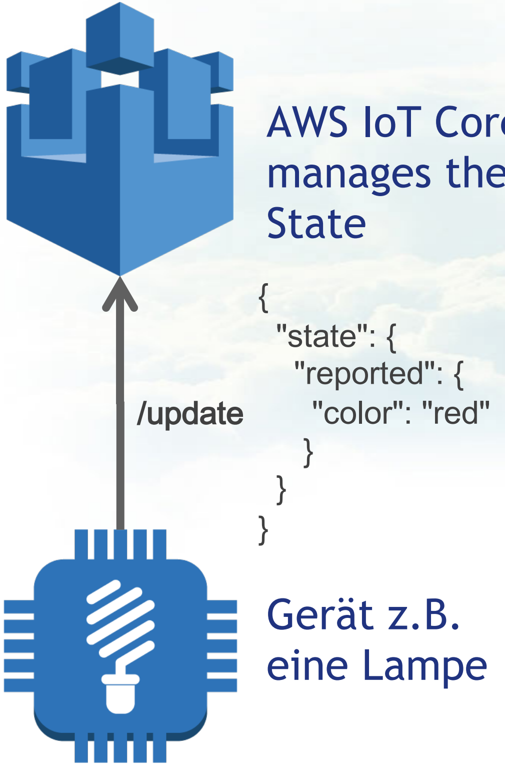
Client A
Broker
Client B
CONNECT
CONNACK
SUBSCRIBE temperature/roof
PUBLISH temperature/roof 25 °C
35
PUBLISH temperature/floor 20 °C
PUBLISH temperature/roof 38 °C
38
DISCONNECT
25
20
38
PUBLISH temperature/roof 25 °C ✓retain
PUBLISH temperature/roof 38 °C

The message broker uses the MQTT protocol. MQTT is also supported via the WebSocket protocol. In the case of an HTTP connection, each action of the server requires a prior request from the client.

With the WebSocket protocol, the connection remains open. The server (broker) can then deliver this open connection new information to the client without waiting for a new connection from the client.

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



```
{
 "state": {
  "reported": {
   "color": "red"
  }
 }
}
```

Device Shadow Services uses reserved MQTT topics to enable applications and devices to retrieve, update, or delete the state information for a device (shadow device).

The names of these topics begin with $aws/things/*thingName*/shadow.

The lamp hereby updates its shadow:
$aws/things/myLightBulb/shadow/update

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

Consumption data are

confidential **and** private

Therefore, we have to look at security...

Protection goals of information security

Confidentiality

Data may only be read by authorized users, both when accessing stored data and during data transmission.

Integrity

Data must not be changed unnoticed. All changes must be traceable.

Availability

prevention of system failures; access to data must be guaranteed within an agreed time frame.

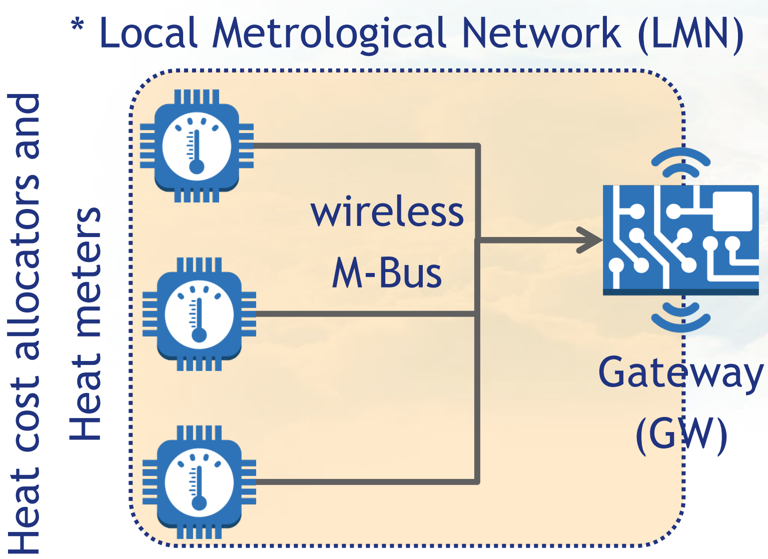
Quelle: https://de.wikipedia.org/wiki/Informationssicherheit

Another overarching goal

Authenticity

Authenticity is understood to mean both proof of identity and the authenticity of the actual data. It is important to ensure that a communication partner is actually who he claims to be.

The measured values must be ...



... encrypted by radio (wireless M-Bus) to the gateway (GW).

Each sensor uses its own 128-bit AES key.

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

The gateway should ...

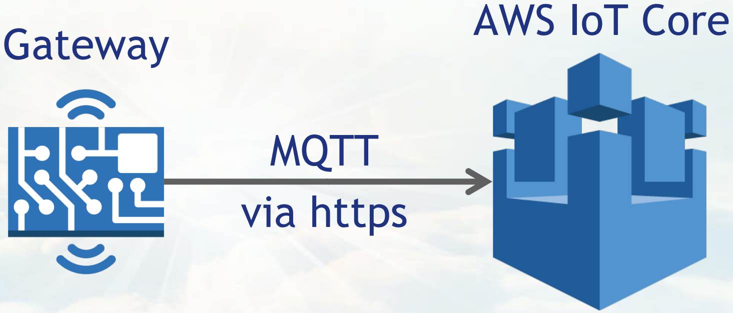


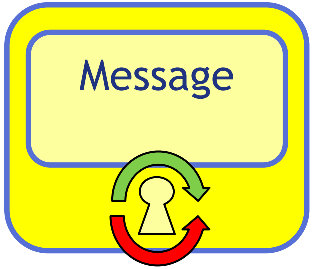
Bild Quelle: https://www.solvimus.de/en/product/muc-one-2/

... the measured values of several sensors in its vicinity are bundled and transmitted to the cloud. The heat cost allocators are connected to the gateway via the wireless M-Bus (LMN). The GW (e.g. MUC.one with its own SIM) transmits the bundled measurement data to the cloud. It handles authorization against AWS IoT Core. Certificates are used for this purpose ...

Inset: Public-Key Cryptography

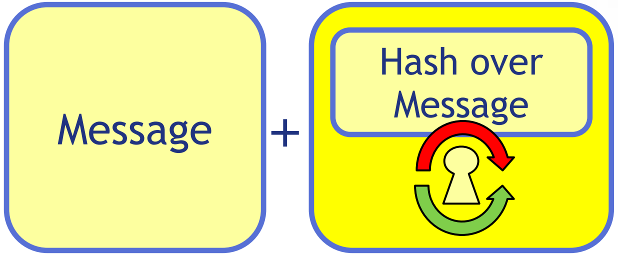
- Basic principle (very briefly)
  - There are two keys (= key pair)
  - What is encrypted with one can only be decrypted with the other (=asymmetric)
  - One key is called public: public key
  - The other key is called private: private key

Asymmetric encryption



Message with
Public Key
of the recipient
encrypted

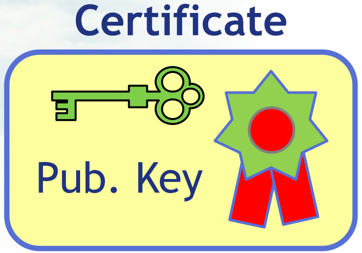
Digital signature



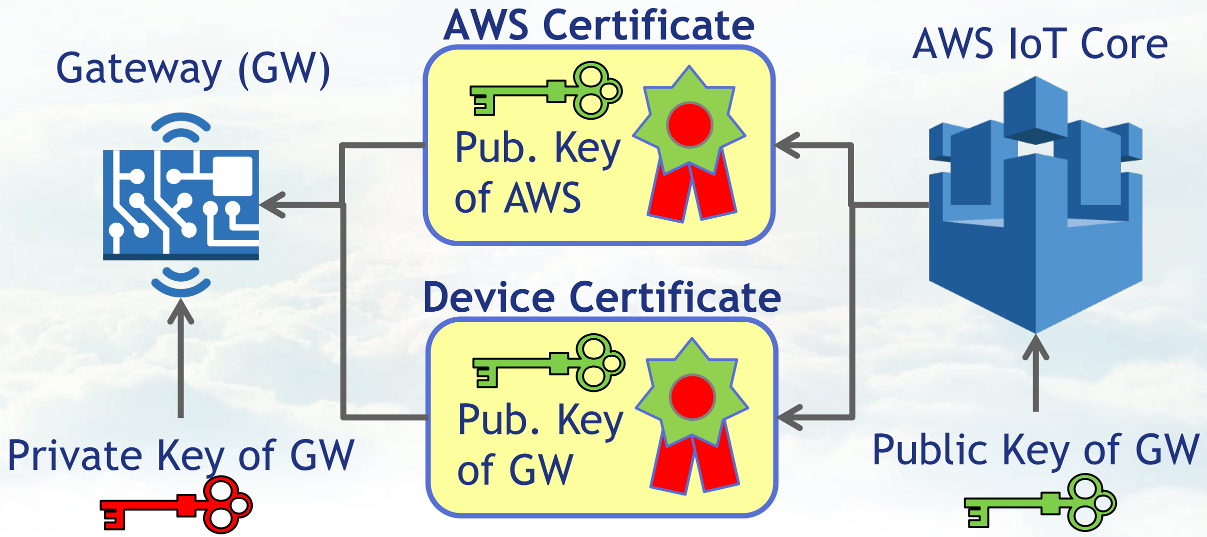
Hash over message with
Private Key
of the transmitter
encrypted

Certificates

- Public keys are exchanged
  - The public key alone should not be trusted
  - It must be signed ("certified") by a third party (CA – Certification Authority)
- The result is called a certificate:
  - Contains the public key and
  - A record about the owner of the key.
  - Both together were digitally signed by the CA
  - AWS has the role of CA in this case
  -

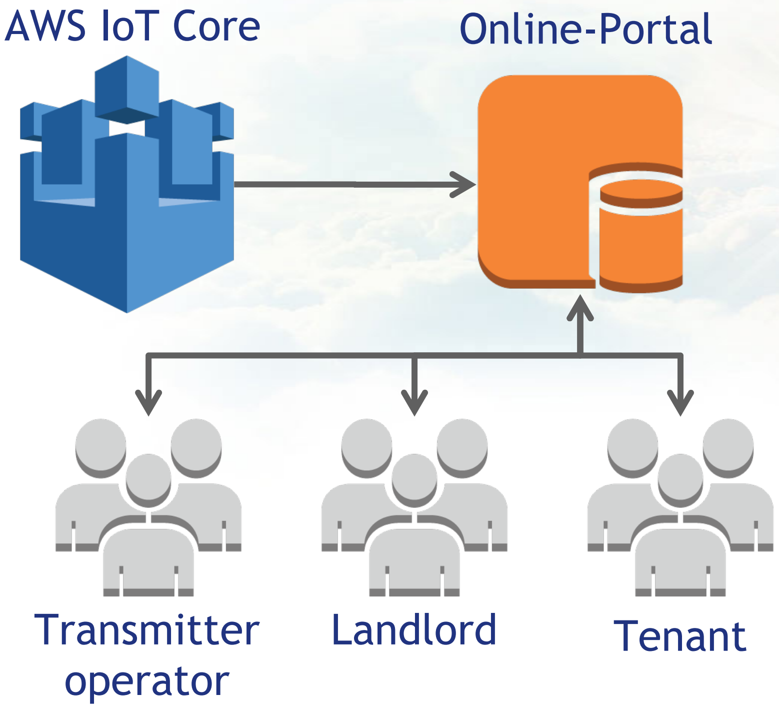


When setting up the gateway …



... Key pairs are created in production using a PKI (Public Key Infrastructure) key pairs. The public key is signed by AWS. This means that AWS creates a specific device certificate from it. In addition, the AWS certificate and the private key are programmed into the gateway. The private key should then be deleted in production.

The online portal ...



... for heating cost billing accesses the measured value data in the AWS IoT Core.

It allows landlords to create consumption-based bills.

It offers tenants a transparent presentation of their consumption data in near real time.

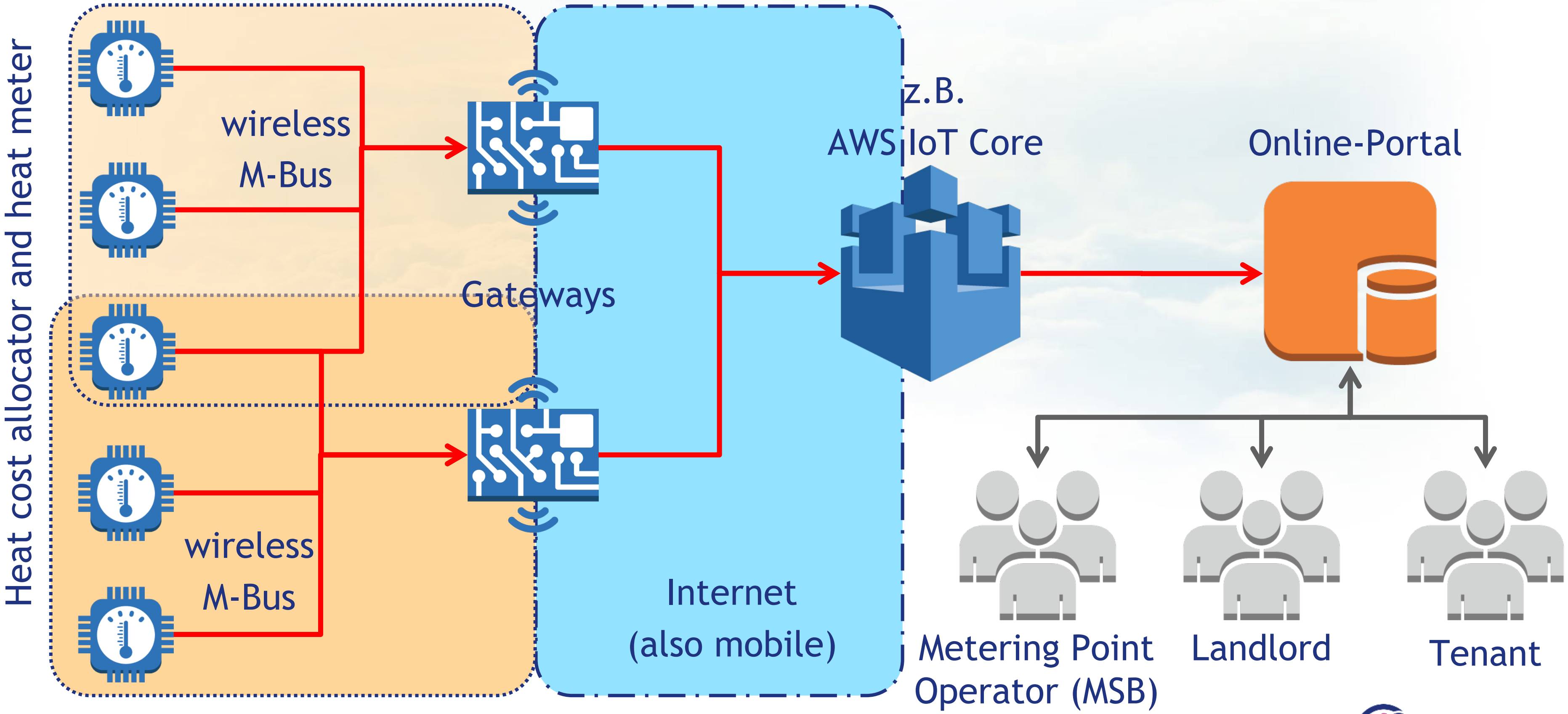
Landlords only see consumption data of their tenants summed up (privacy!)

Metering point operators use this to manage heat cost allocators and gateways.

What do we do differently?

- No smart meter gateway
- Readings are not decrypted in the gateway
- Only the online portal knows the keys of the heat cost allocators
  - This makes it easier to set up the gateways
  - AWS IoT Core does not have access to private data!
- Separation of AWS IoT Core and online portal

Measured values remain encrypted



Discussion of some attack scenarios

- Listening to the M-Bus radio channel
  - Possible but ineffective
- Replay of meter readings
  - Not possible. Counter provides individual telegrams
- DoS, radio channel overload
  - Possible but damage manageable
- Manipulating counters
  - Counters have tamper detection
- Clone gateway by reading the private key
  - Ineffective if you don't clone the counters as well
- Man-in-the-Middle (zwischen Gateway und AWS)
  - Prevented by certificates
- Meter keys are stolen from portal
  - Theoretically, not really preventable. Protected by standard security measures

Announcement

- Partnership between 4FO and solvimus
  - 4FO develops and operates an online service for solvimus
  - solvimus launches the online service under its own name
  -

Outlook

- Internationalization
- Water supply
  - is precious in many regions of the world
- Monitoring-System
  - With 15min measuring intervals, a burst water pipe can be detected quickly
  -

Thank you very much

CEO, Dr. Jürgen Nützel

4FriendsOnly.com
Internet Technologies AG