Reference: Hans Blossey, Forschungslinie Licht_Raum, FH Dortmund

Smart Energy IoT Applications - Services and Security Aspects

Institute of Communications Technology and Signal Processing

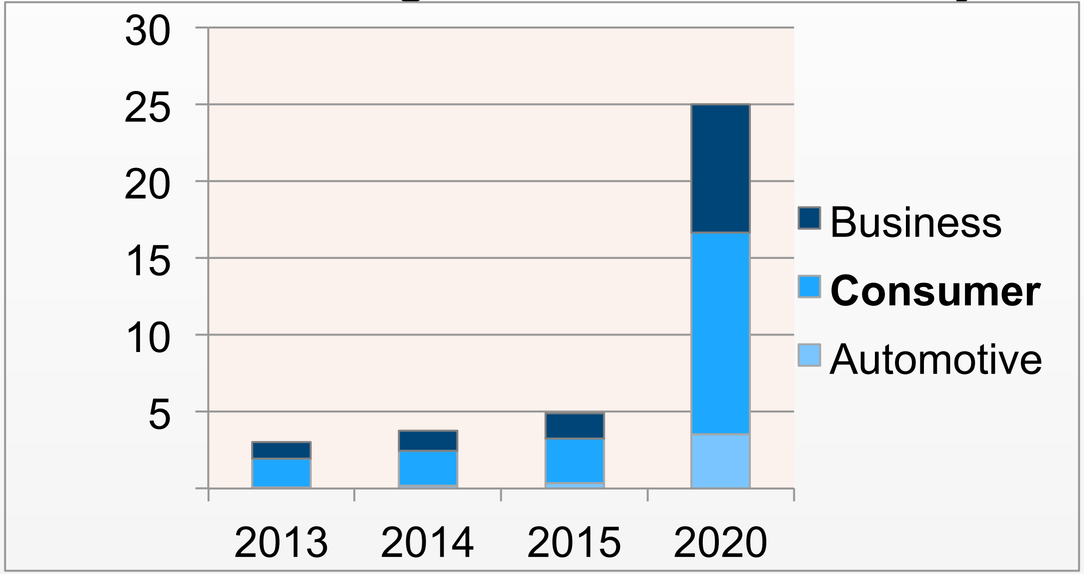
Prof. Dr. –Ing. Ingo Kunold , M.Eng. Marco Niemeyer

www.ikt-dortmund.de

Internet of Things (IoT)

Ruhr Master School of Applied Engineering

Internet of Things units installed base by category (in billions) worldwide*



Reference: Gartner,Inc. November 2014

*Excluding PCs,tablets and smartphones

A forecast expects in 2020 over 25 billion connected „things“

Important tasks of the Internet of Things are

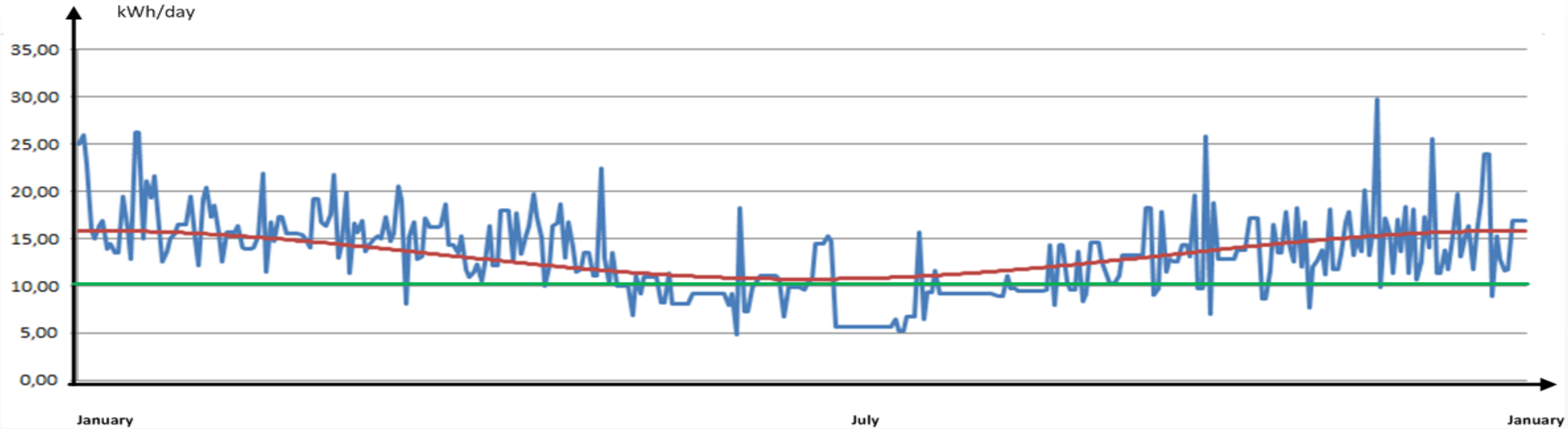
Smart Building and
Smart Energy Services with
→M2M/M2H communication
→ Deployed on
embedded hardware platforms

Some Interests of energy data aquisition

Todays power supply with regenerative systems is more volatile and the price for power depends on its availability.

- **Power suppliers** need to define new time depended energy tariffs and the corresponding billing.
- **Power suppliers and producers** are working of concepts for load balancing in volatile power networks.
- **Power consumers** are interested to their detailed power consumption behavior and in their potential to save energy without loss of comfort.
- **Housebreakers** are interested lo learn at what time people are on holidays or at work.
- **Spies** are interested in any kind of personal data to get vitreous people.

Detection of individual classification data over an anual period

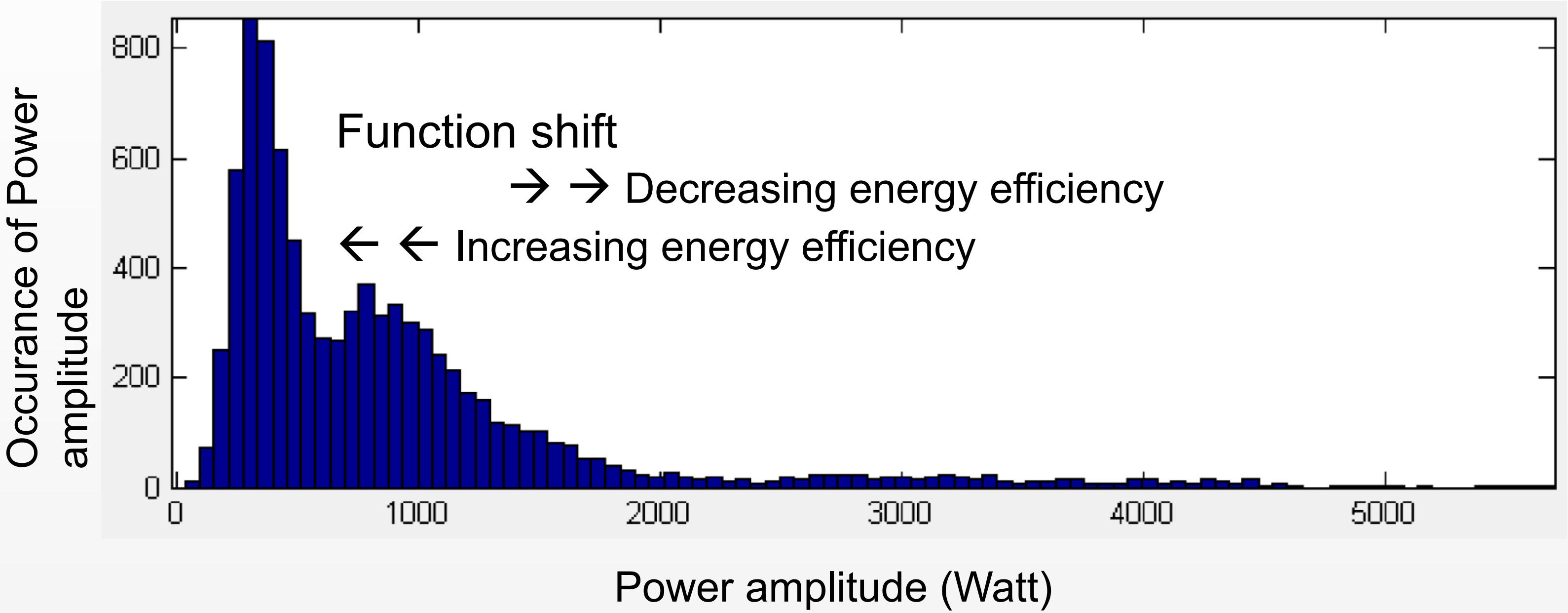


Example of an annual profile of power consumption of a one-family house

- ----- : measured daily power consumption
- ----- : fundamental wave of power consumption (cosine function with anual period and magnitude p_{mag})
- ----- : daily base load (offset) p_{min}

Sep. 2015 - © IKT FH Dortmund

Detection of commonly used power consumption (devices)



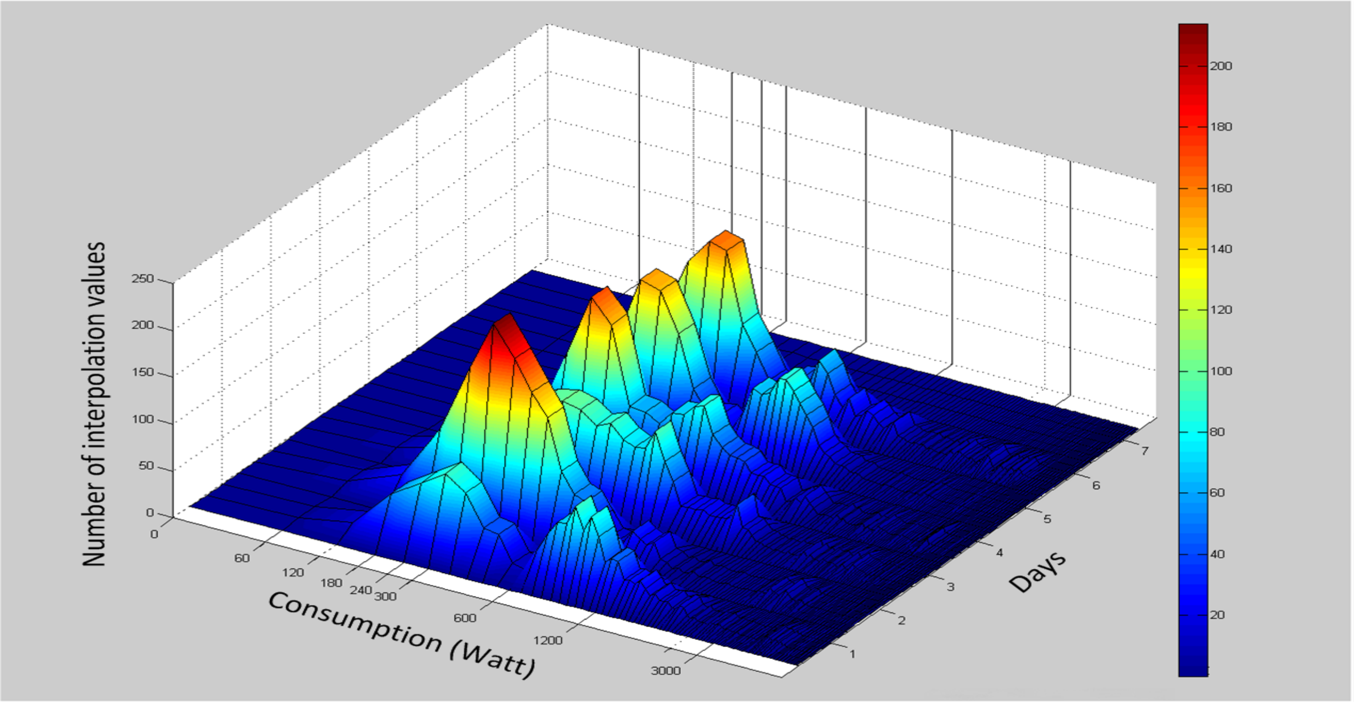
Function shift

→ → Decreasing energy efficiency

← ← Increasing energy efficiency

Relation of different power amplitudes in a weekly observation interval

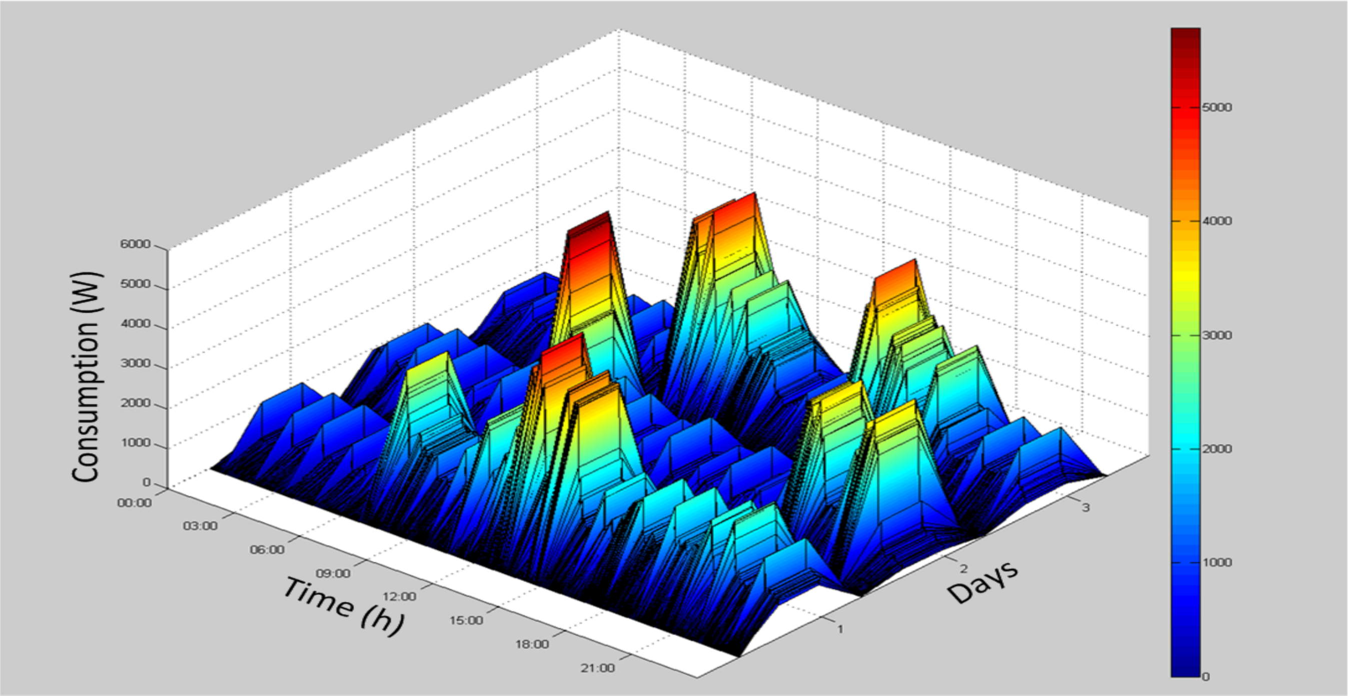
Commonly used power consumption during a week



Comparing frequency scale view

Daily power load profiles of 3 different typical days

Ruhr Master School of Applied Engineering



Comparison of daily load profiles

Basic Principles of Internet Security

General security threats from the internet are:

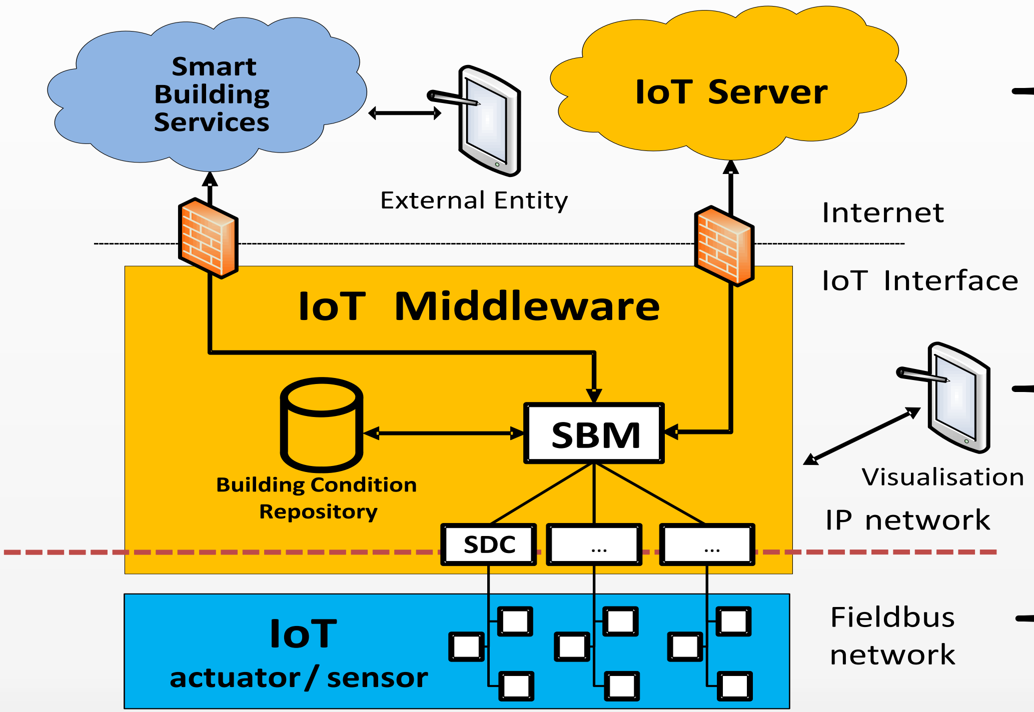
- The system can be entered or taken over (Hacking).
- Sensitive data from the systen can be stolen or spied out.
- Access to the system can be prevented or sensitive data can be deleted.
- Data can be modified or falsified.
- To get access to the system a false identitiy can be pretended.

Primary goals of internet security are to make sure the

- **Confidentiality** → Information is only for authorized entities availiable
- **Integrity** → means accuracy, consistency and completeness of data
- **Availability** → Information is available when it is needed

A Smart building system (SBS) approach - IoT system architecture

Ruhr Master School of Applied Engineering



IoT Server as backend system

- Long term status/data storage

Different Smart Building Services

(e.g. control/supervision/prediction)

Smart Building Manager SBM

- Proxy features
- Providing near real-time status/data exchange
- Local smart service engine

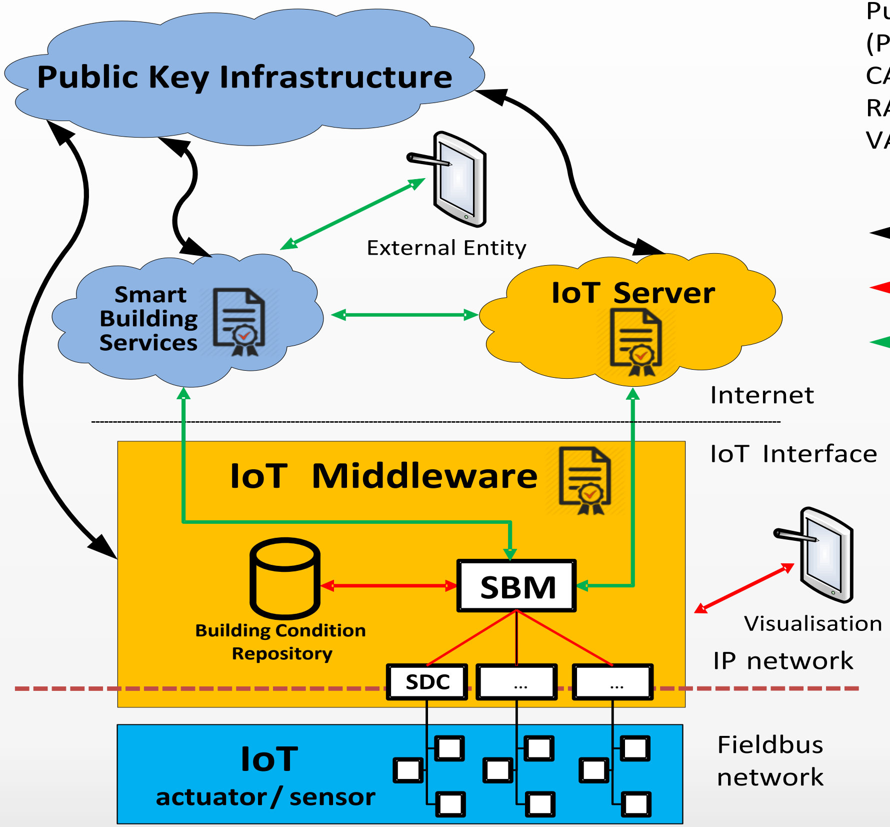
Smart Device Controller SDC

- Mapping of fieldbus protocols to a uniform data structure

Support of different fieldbus protocols

Sep. 2015 - © IKT FH Dortmund

A Smart building system (SBS) approach - IoT security architecture



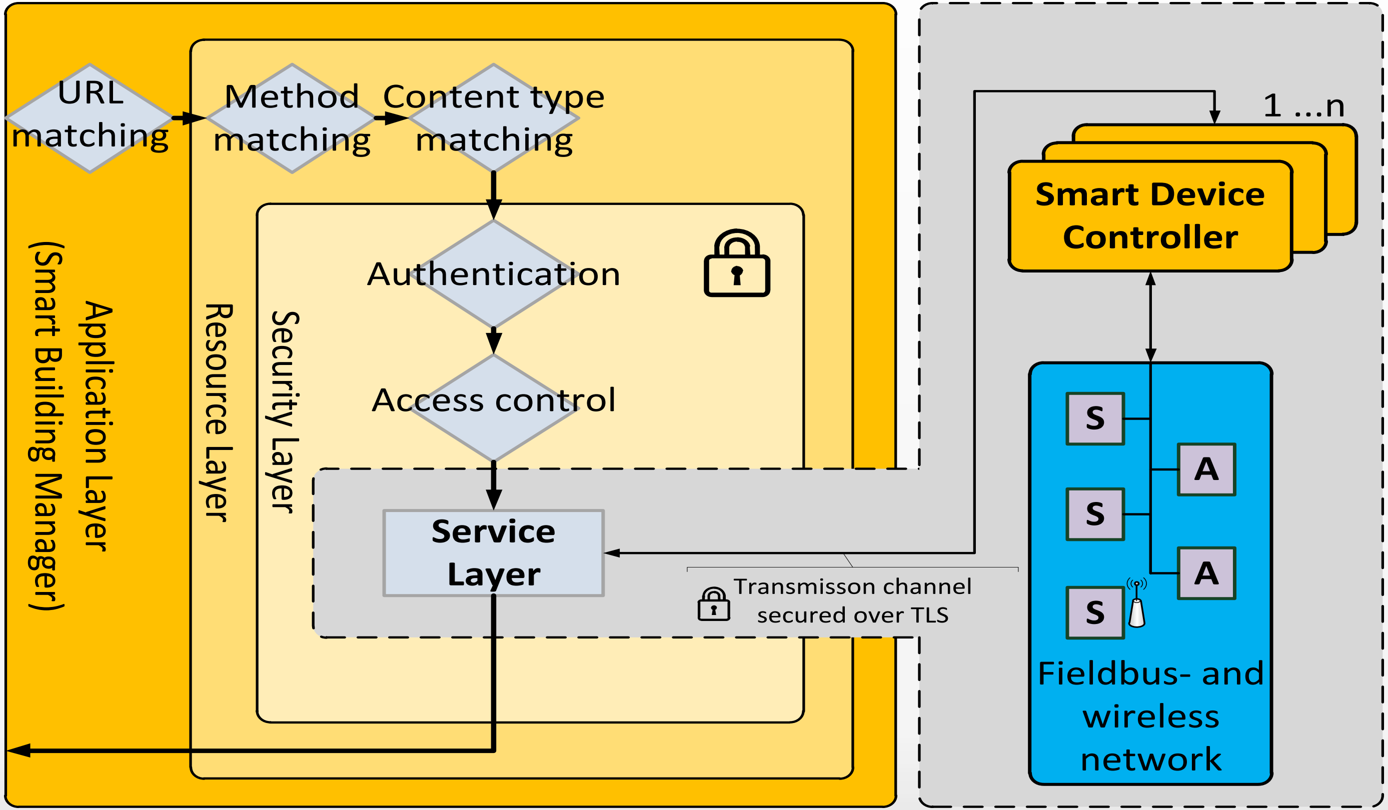
Public Key Infrastructure (PKI) :
CA: certification authority
RA: registration authority
VA: validation authority

↔ Certificate exchange and validiation

↔ Unsigned TLS certificate

↔ Signed TLS certificate

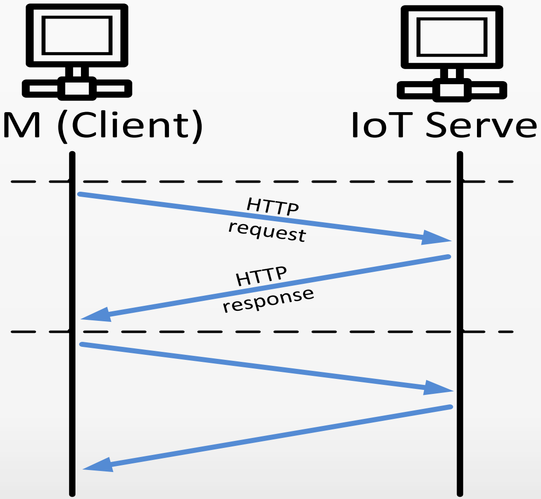
Processing a HTTP request on the SBM



Standard communication procedures using Transport Layer Security TLS

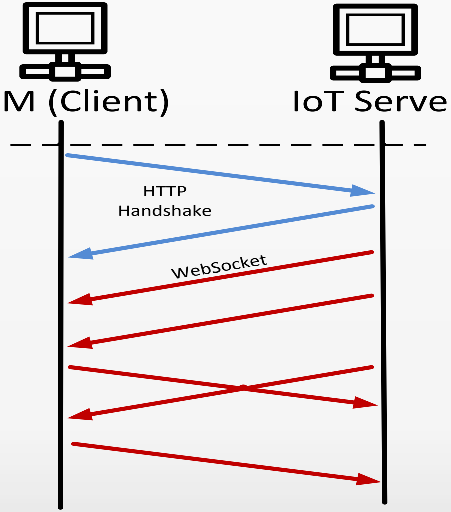
RESTful Web Services

REST is a common architectural style and widely used for web-based M2M communication

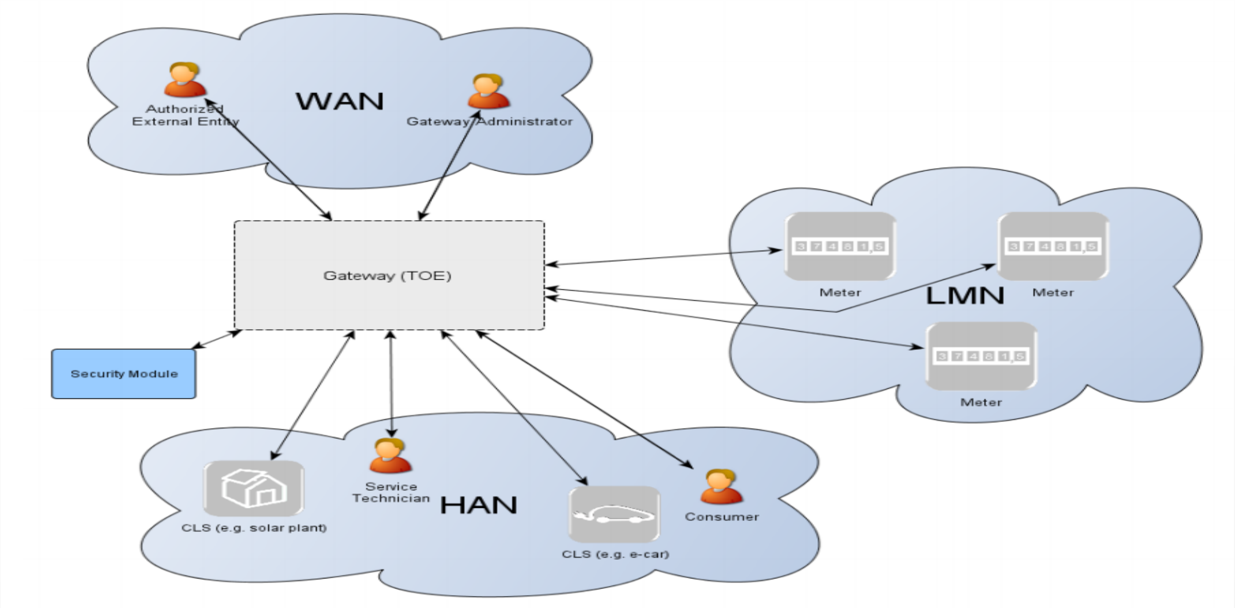


WebSocket technology

With the WebSocket protocol an event based messaging can be realised over a single TCP channel. The data is exchanged bi-directional and full-duplex.



Security in a smart metering system



Logical Interfaces of the Smart Meter Gateway

Sep. 2015 - © IKT FH Dortmund

Security in a smart metering system

The German Federal Office for Information Security (BSI) has defined the Protection Profile BSI-CC-PP-0073 along with the technical guideline TR-03109. This defines the requirements for a Smart Meter Gateway (SMGW) and its interaction with other components in a smart enviroment.

BSI TR-02102-2 defines the use of Transport Layer Security (TLS)

The approach is to minimize weak points of potential attacks

→ Generally every communication channel must be secured by TLS

→ Only data traffic between a SMGW and authorized external entities (e.g. smart energy services)

→ Mutual authentication (server/client) to prevent Man-in-the-middle attacks

Measures to protect a smart energy system

Prevention of entering or takeover of a system (Hacking):

- An entity authenticates itself to the system
- With a mutual authentication with certificates for every instance (server/client) the Man-in-the-middle attacks can be prevented
- An entity has only access to the system with a valid, randomly generated session token

Prevention of spy out or steal data

- The transmission channel is encrypted by Transport Layer Security (TLS)
- Unauthorized acccess to the system is prevented by use of a role based Acess-Control-List (ACL)

References

[1] M. Kuller, I. Kunold, H. Hoffmann „*Middleware- und Visualisierungskonzepte für Smart-Energy-Systeme“ aus Smart Energy 2013- Wie smart ist Deutschland im europäischen Kontext*. vwh | Verlag Werner Hülsbusch, ISBN: 978-3-86488-055-1, November 2013, pp. 42 – 55.

[2] BMWi - Federal Ministry of Economics and Technology, “GUDED AB,” 2013-2016. [Online]. Available: http://-www.guided-ab.de/-

[3] BSI - Federal Office for Information Security, “Protection profile for the gateway of a smart metering system,” 2014.

[Online]. Available: https://-www.bsi.bund.de

[4] BSI - Federal Office for Information Security, “BSI TR-03109,” 2012. [Online]. Available: https://-www.bsi.bund.de

References

[5] BSI - Federal Office for Information Security, “BSI TR-02102-2” 2014. [Online]. Available: https://-www.bsi.bund.de

[6] T. Garn, “Realization of a signal processing system for energy efficiency analysis of smart metering data with Matlab and Java,” Master’s thesis, University of Applied Sciences and Arts Dortmund, Germany, 2011.

[7] M. Niemeyer, K. Henneböhle, M. Kuller, I. Kunold, “Security requirements of IoT-based smart buildings using RESTful Web Services,” in *30th International Kandó Conference on 20th November 2014*. Budapest, Republic of Hungary: Óbudai University, November 2014.

Quelle: Hans Blossey, Forschungslinie Licht_Raum, FH Dortmund

Thank you for your attention.