Hochschule Offenburg
offenburg.university

SMI
Smart Meter Inclusif

ivESK
Institut für verlässliche Embedded Systems und Kommunikationselektronik

“Practical security analysis of German smart metering systems ”

28th September 2021

Rigoev, Ivan, M.Sc.

About SMI - Smart Meter Inclusif project

SMI
Smart Meter Inclusif

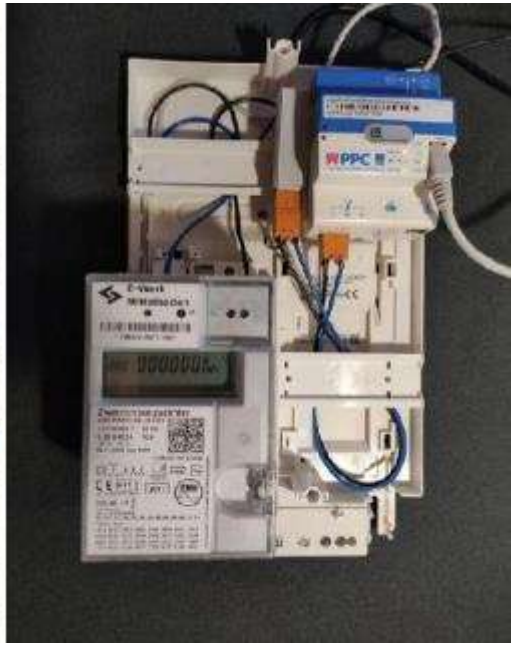
Artificial intelligence to support the **proactive management of energy consumption** by **end users**

Our part of SMI project

Work package 4: Security concepts for distributed Smart Grids

4.1. Comparative security analysis

4.2. SMI solutions penetration testing

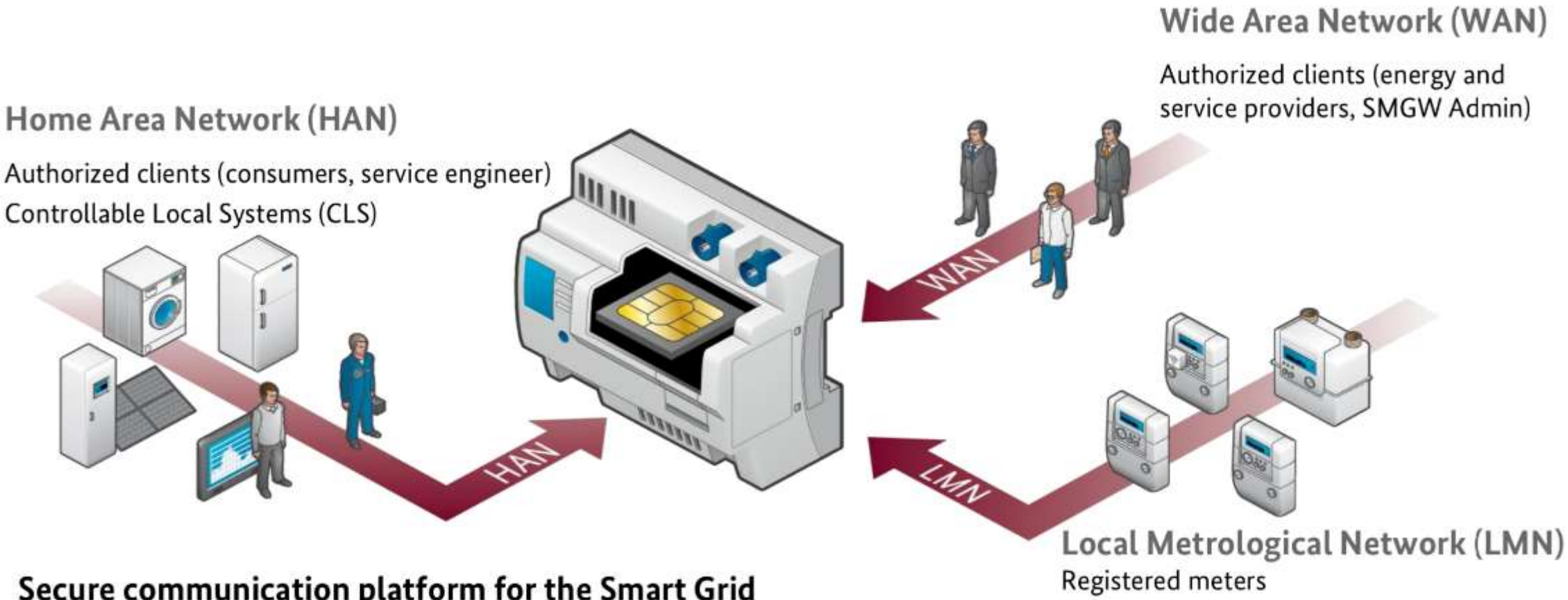




German SMI systems

Federal Office
for Information Security

- BSI is commissioned by Federal Ministry for Economic Affairs and Energy
- Technical standards have been developed by the BSI together with industry, federal associations, Federal Data Protection Commissioner, Federal Network Agency and National Metrology Institute

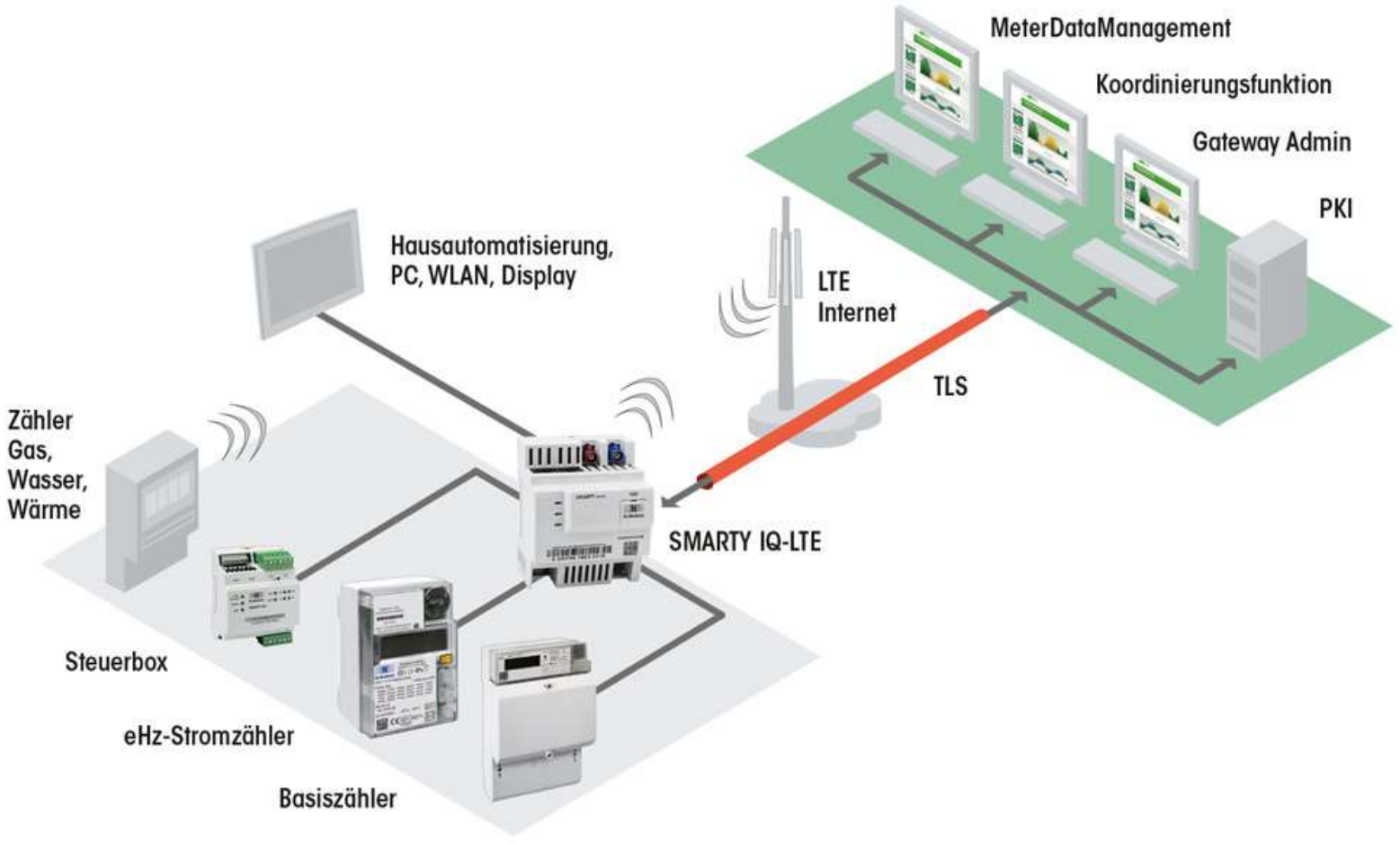
SMGW - Smart-Meter-Gateway



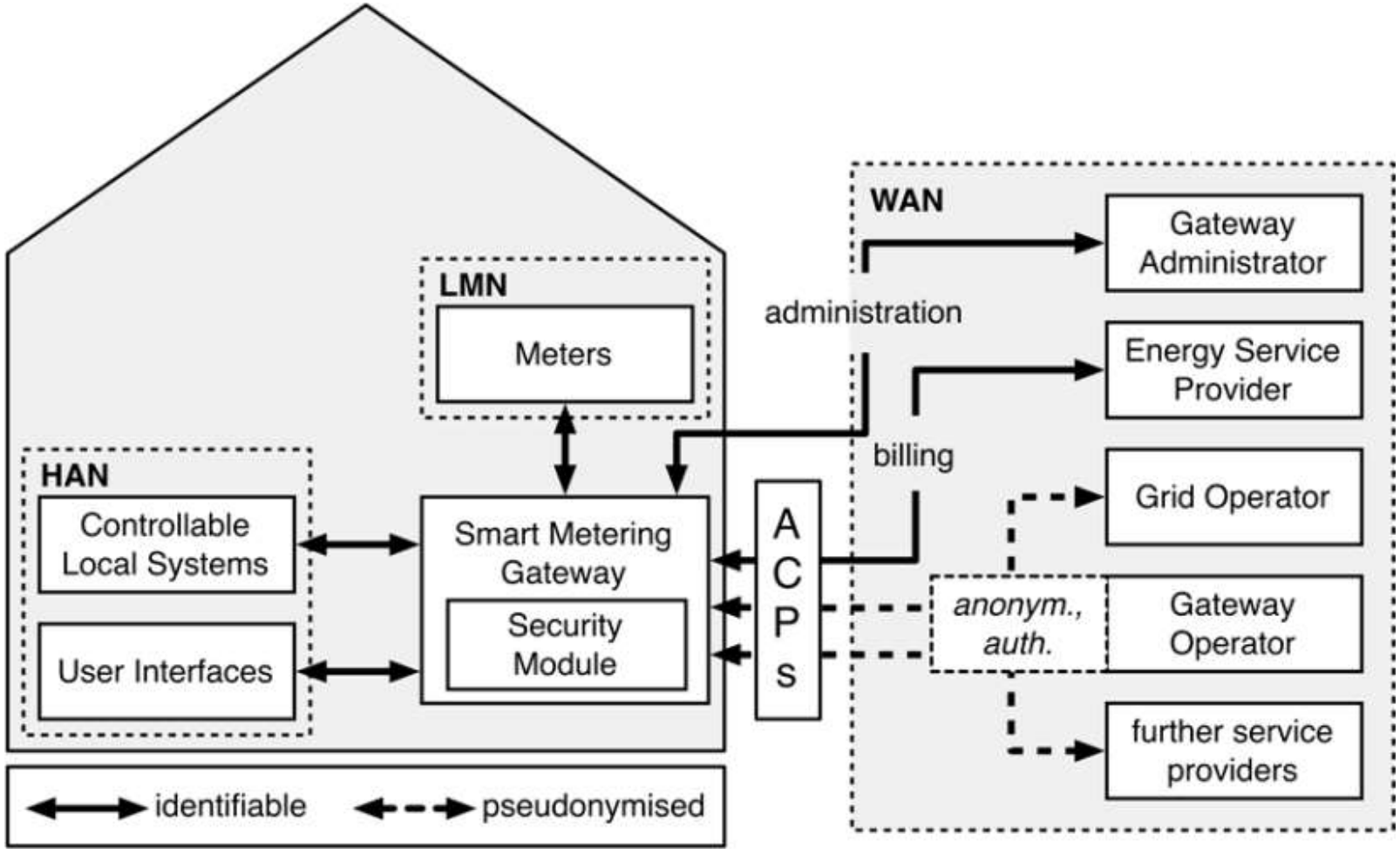
Secure communication platform for the Smart Grid

- Transparency of consumption data and privacy compliant transfer of measured data
- Control of consumption and power generation units (load / feed-in management)

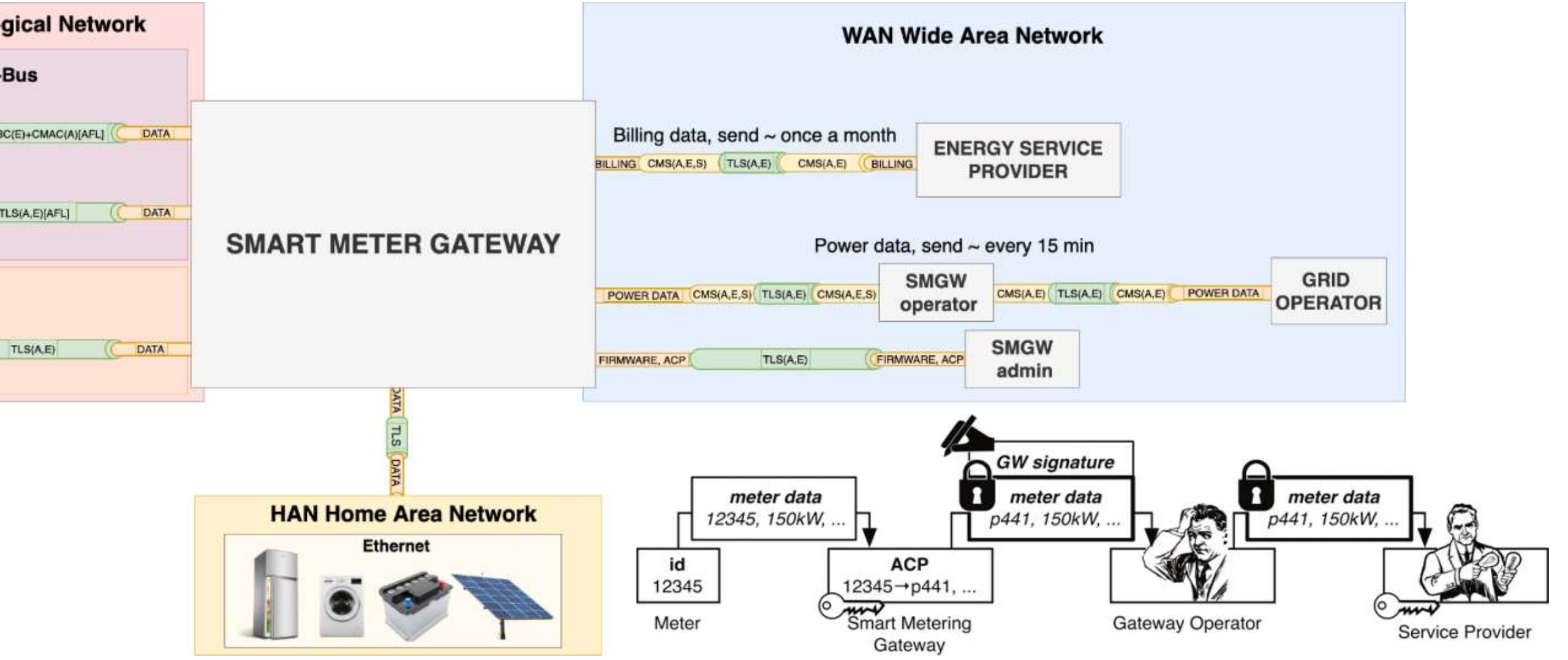
SMGW smart metering system architecture



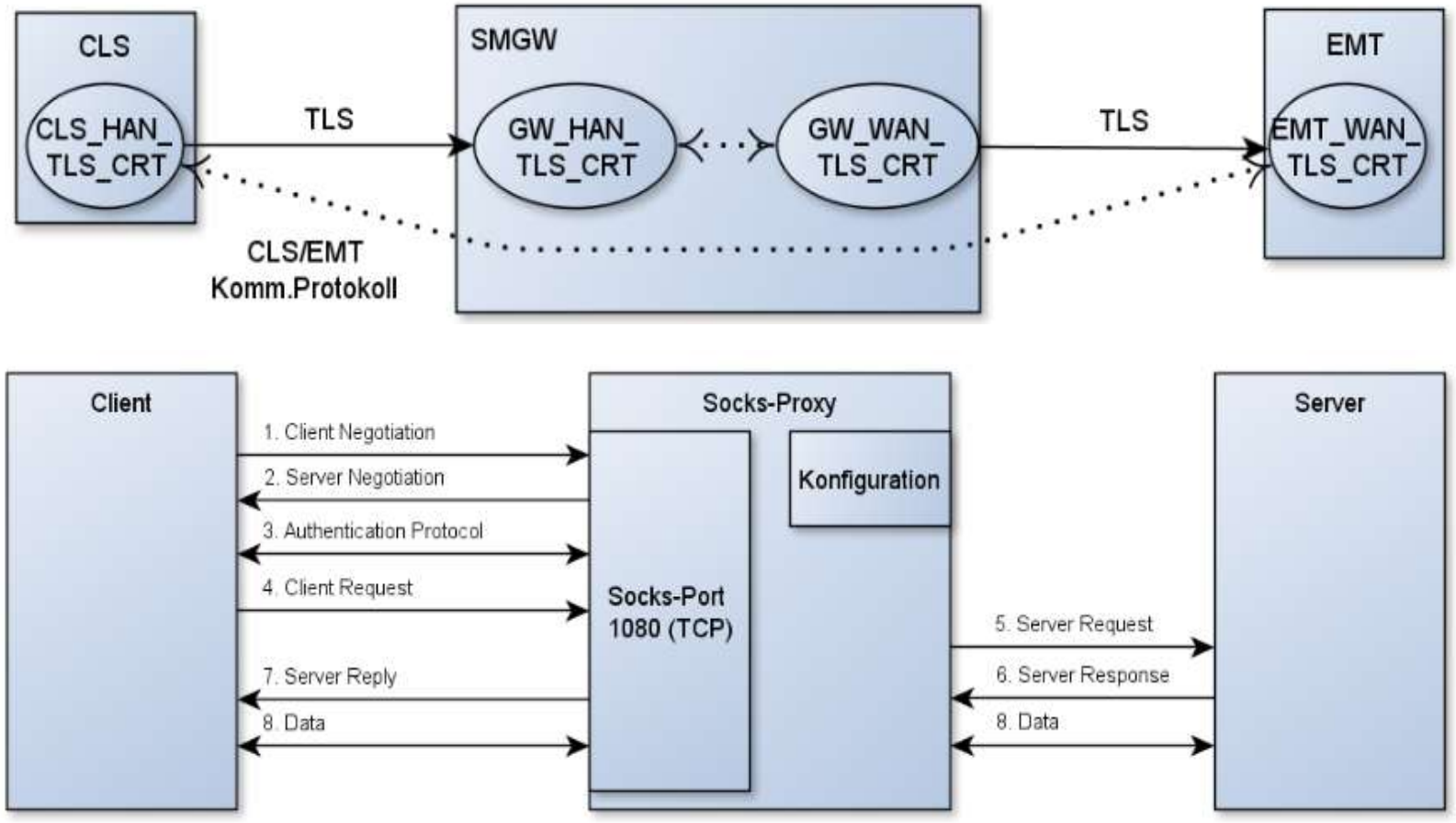
Market participants, their tasks, and types of data



WAN communication

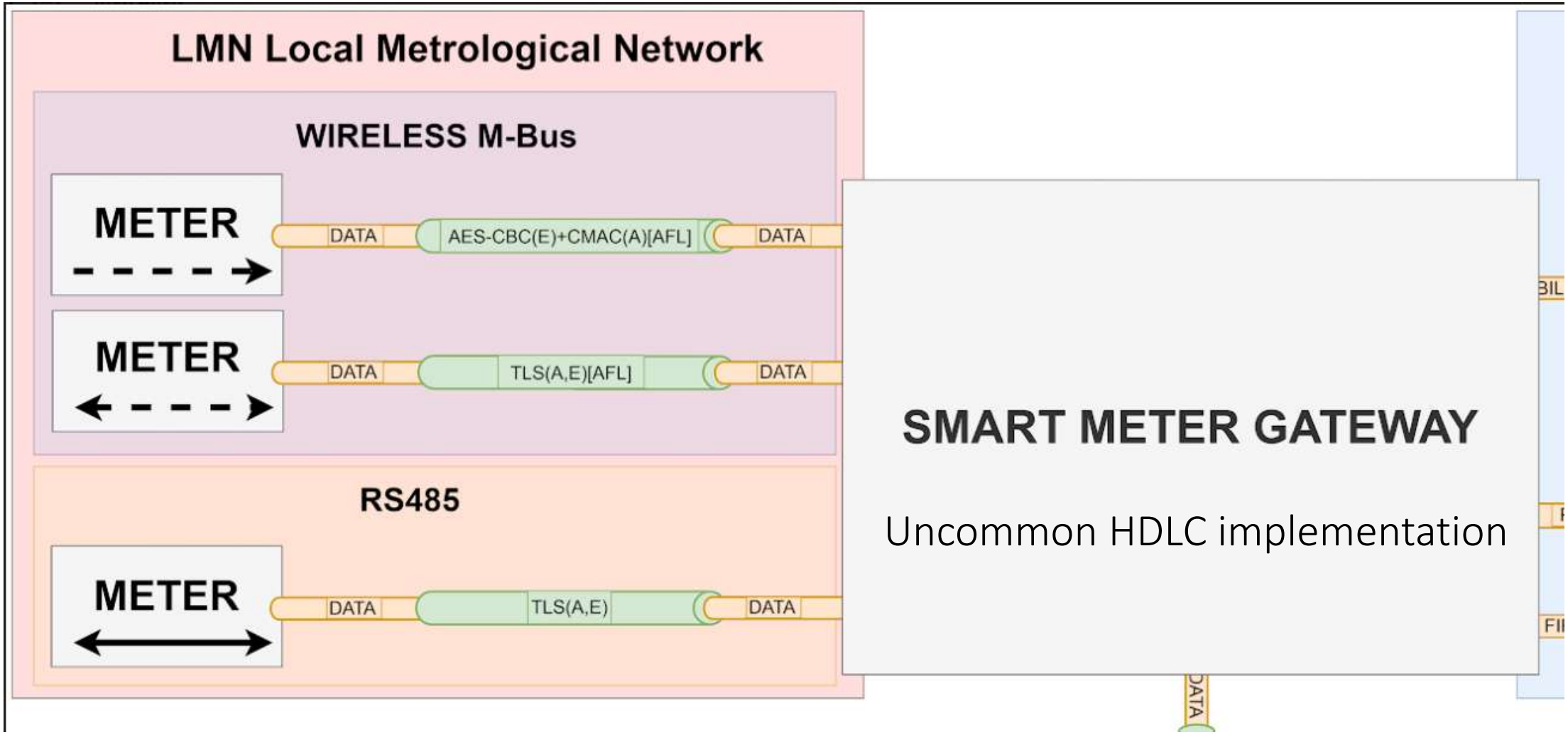


HAN communication scenarios



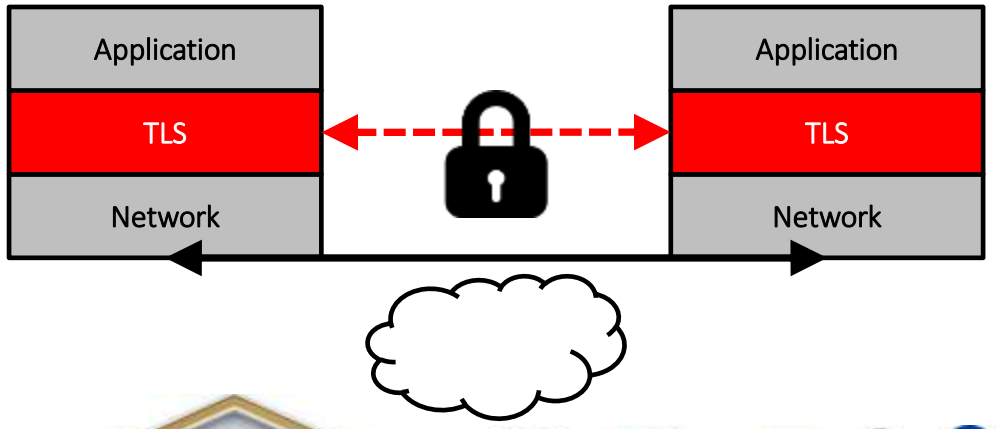
- HKS1: Bidirectional communication in the HAN with authentication using HAN certificates (service)
- HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and password
- HKS3: Transparent channel initiated by CLS
- HKS4: Transparent channel initiated by EMT
- HKS5: Transparent channel initiated by SMGW

LMN communication

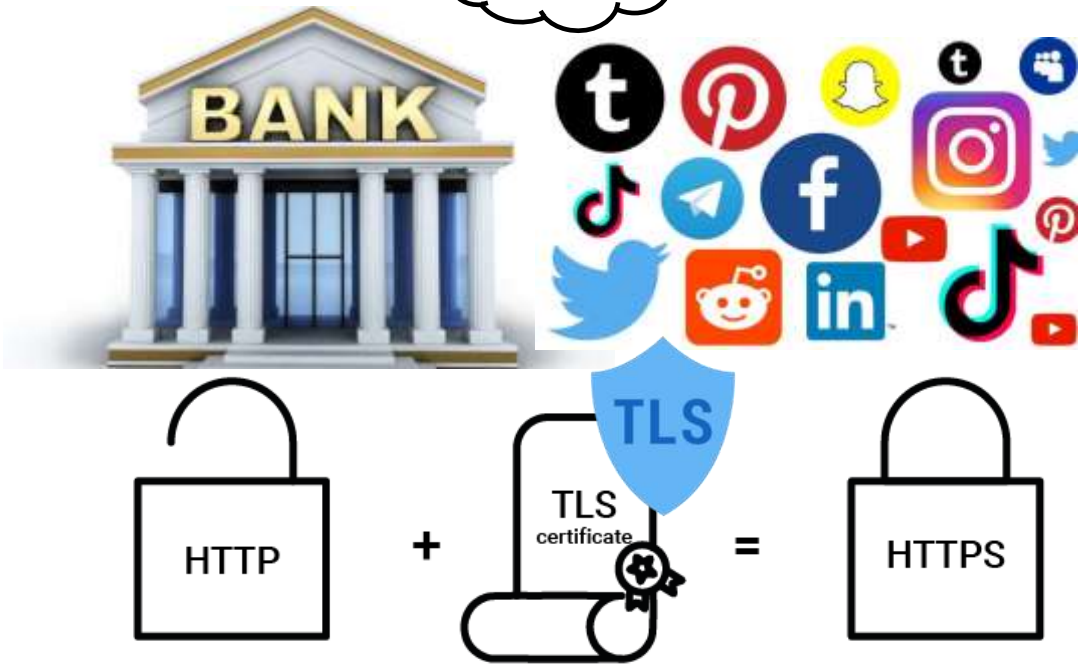


Transport Layer Security (TLS)

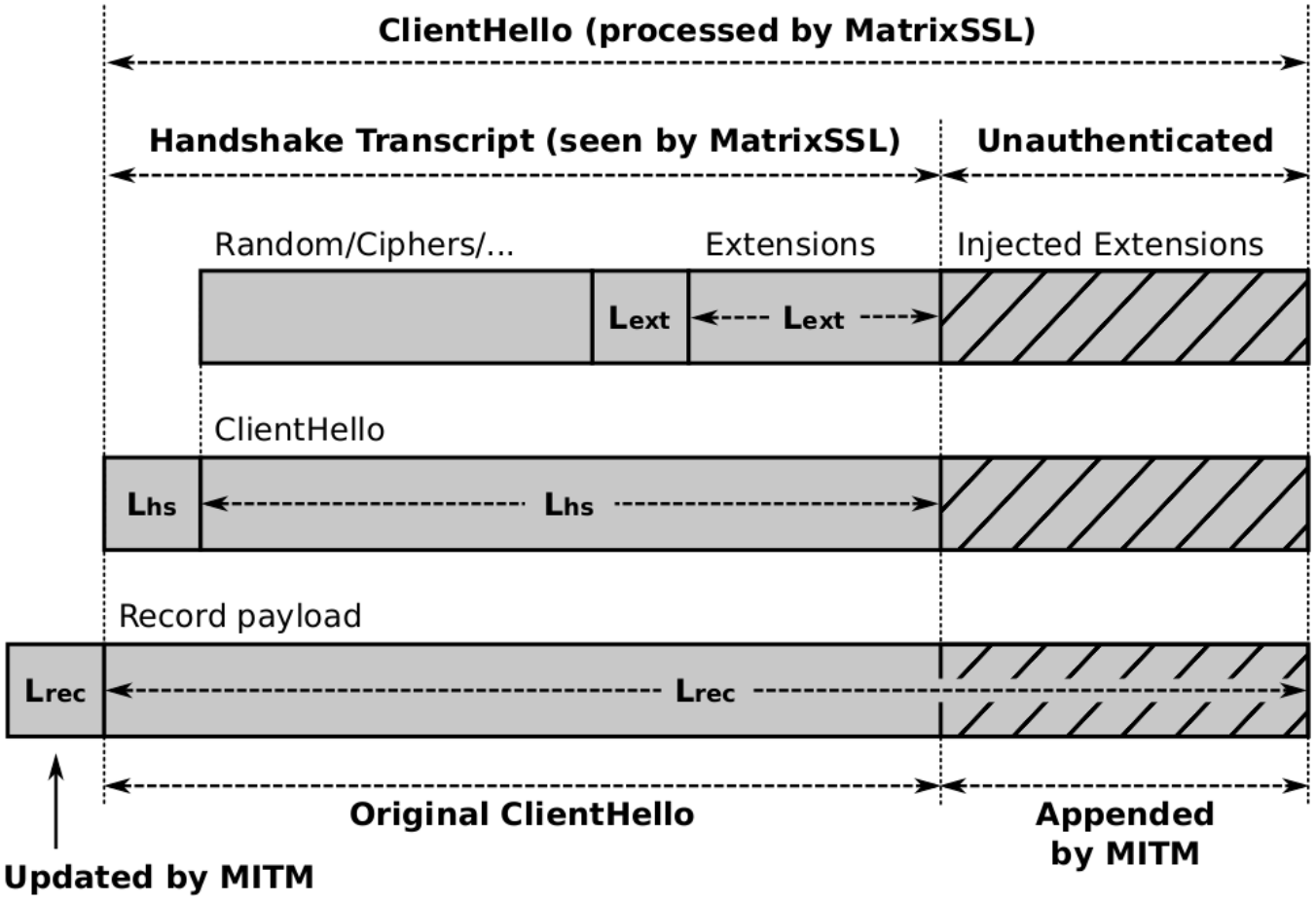
- TLS = Transport Layer Security
  - Client/server protocol
  - End-to-end security
  - Authenticity, confidentiality, integrity

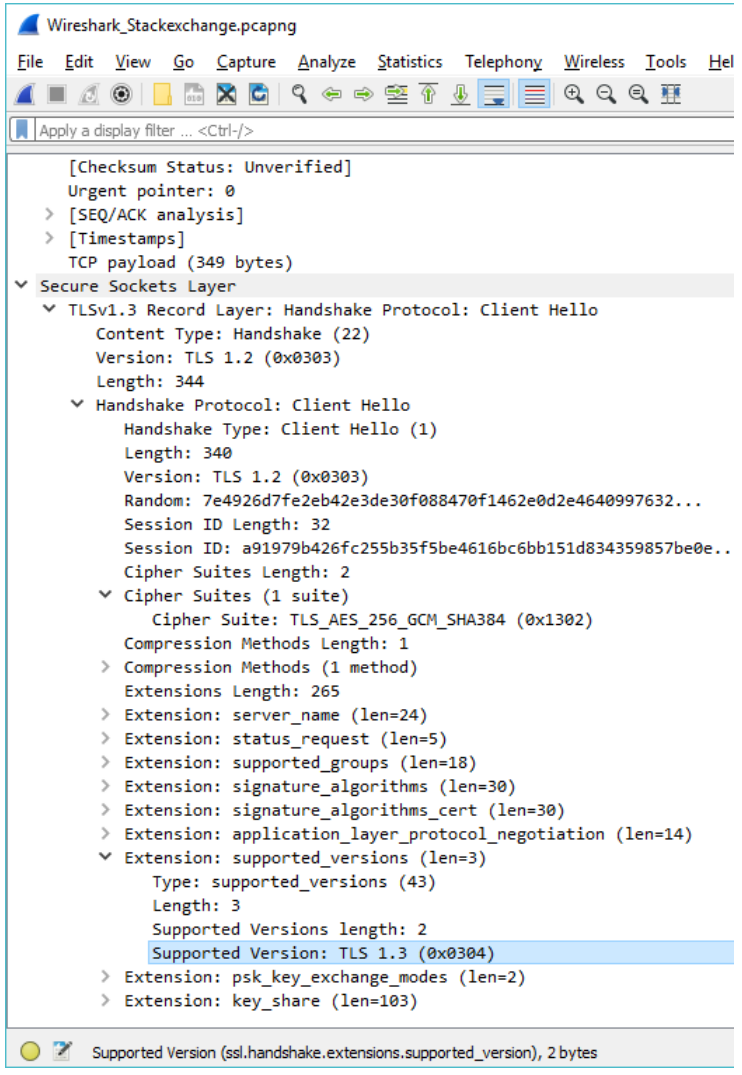


- The TLS protocol is complex
  - Specified in more than 80 non-formal documents (RFCs)
  - Complex protocol messages with deep nesting
  - Rich parameter space (versions, ciphers, extensions, optional features, …) with dynamic negotiation

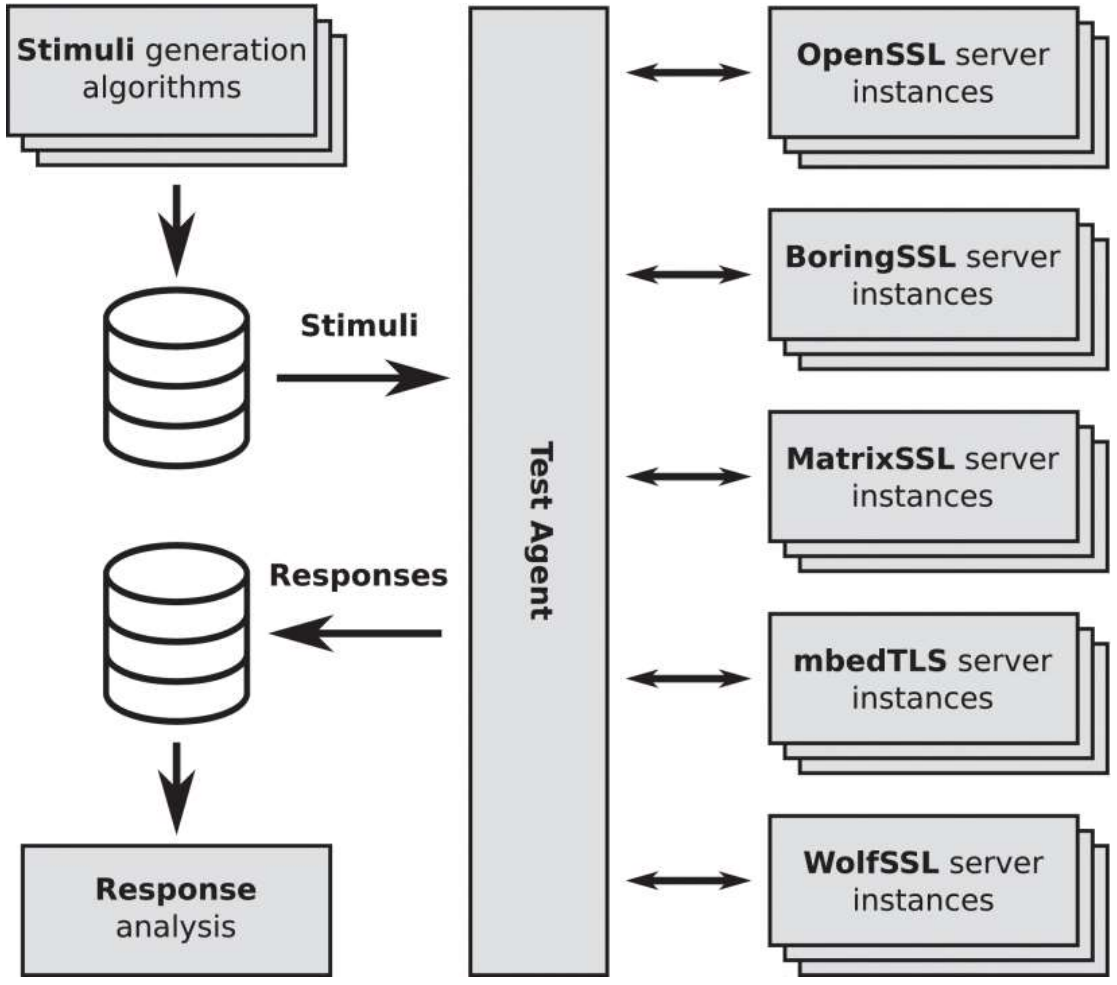


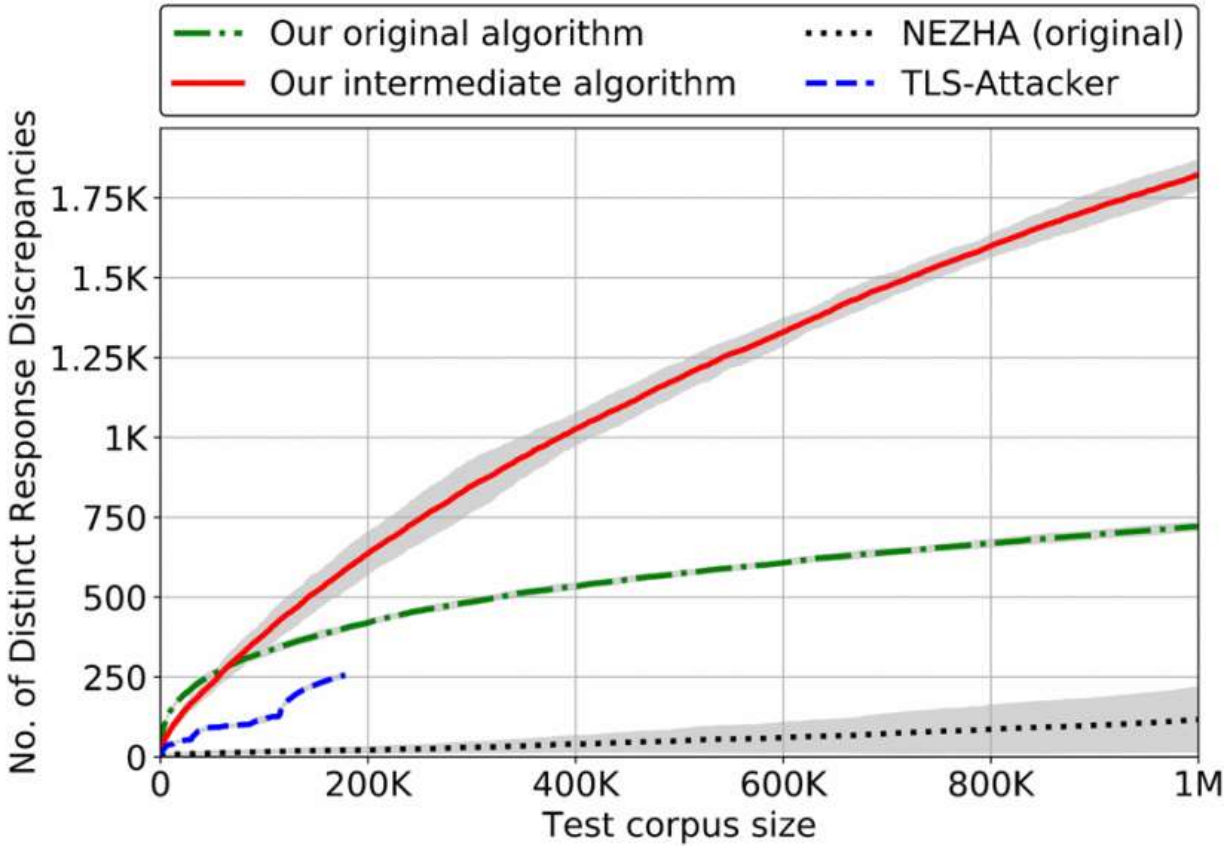
Fuzzing technology



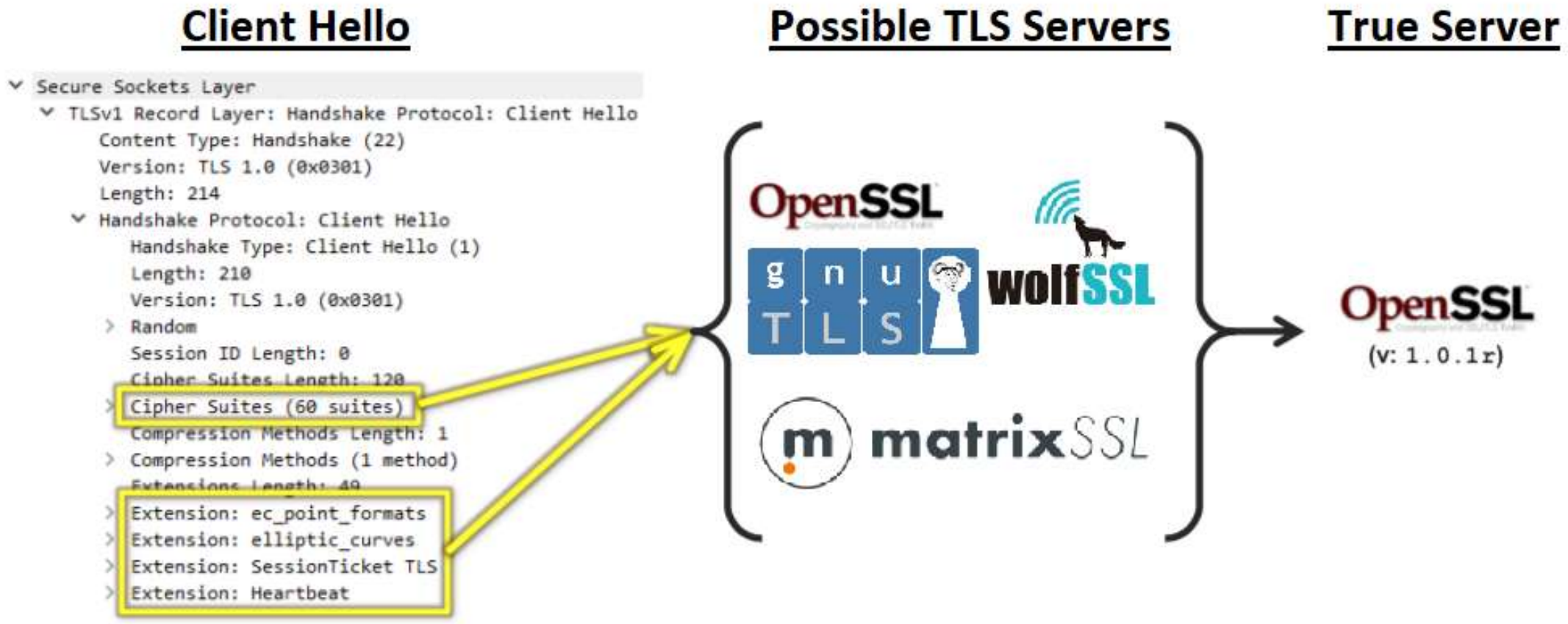


New TLS server fuzzer based on Response-Guided Differential Fuzzing approach





TLS implementation fingerprinting



PPC and conexa SMGW testing results

PPC SMGW

- HAN TLS server implementation GNUtls 3.7.x
- Have working SSH with (public key, password) authentication
- Got SSH user list via malformed package technique (checked on raspberry pi with same dropbear SSH 2017.75)
- Tried different brute force software – hydra is the most fast in this case
- Tried 14 344 407 passwords (in more than 2 months). None is correct

Conexa SMGW

- HAN TLS server implementation mbedtls in range of versions from 2.7.x-2.24.x
- Documented Socks5 for HKS3. Accept only “Secure Sockets Layer for SOCKS Version 5” authentication.
- Find undocumented fuzzing protection (tcpwrapped after 25 incorrect TLS client hello messages.

Other possible attacks. ARP spoofing + MITMproxy for HKS2

victim PC

IP: 192.168.0.10
MAC: [aa:aa:aa:aa:aa:aa]

SMGW HAN TLS server

IP: 192.168.0.164
MAC: [bb:bb:bb:bb:bb:bb]

HKS2: Bidirectional communication in the HAN with authentication using a unique identifier and password

attacker macbook

Modified ARP Cache Points
IP: 192.168.0.164 to
MAC: [cc:cc:cc:cc:cc:cc]

Modified ARP Cache Points
IP: 192.168.0.10 to
MAC: [cc:cc:cc:cc:cc:cc]

IP: 192.168.0.56
MAC: [cc:cc:cc:cc:cc:cc]

Current work. LTE WAN traffic sniffing

CMW500 wideband radio communication tester and 2 other SDR LTE base stations

Raspberry pi with LTE hat

Future plans. Use registered for CLS socks5 proxy to connect to EMP network

CLS – controllable local system

SMGW

External market participants

Thank you for your interest

Hochschule Offenburg
offenburg.university

Ivan Rigoev

Scientific Employee
Institute of Reliable Embedded Systems and Communication Electronics

Telefon +49 (0)781 205-4713
Fax +49 (0)781 205-45 4713
saeed.abdolinezhad@hs-offenburg.de

Badstraße 24
77652 Offenburg
www.hs-offenburg.de

Hochschule Offenburg
offenburg.university

Heiko Bühler M.Sc.

Institute of Reliable Embedded Systems and Communication Electronics

heiko.buehler@hs-offenburg.de

Badstraße 24
77652 Offenburg
www.hs-offenburg.de

Hochschule Offenburg
offenburg.university

Prof. Dr.-Ing.
Axel Sikora Dipl.-Ing. Dipl.-Wirt.-Ing

Scientific Director
Institute of Reliable Embedded Systems and Communication Electronics

Telefon +49 (0)781 205-416
Fax +49 (0)781 205-45 416
axel.sikora@hs-offenburg.de

Badstraße 24
77652 Offenburg
www.hs-offenburg.de

Hochschule Offenburg
offenburg.university

Andreas Walz

Institute of Reliable Embedded Systems and Communication Electronics

andreas.walz@hs-offenburg.de

Badstraße 24
77652 Offenburg
www.hs-offenburg.de

- All currently found vulnerabilities belong to the systems information disclosure (no remote code execution, data tampering).
- Consumption data sniffing in HAN is possible only when hackers intrude on a local network.
- Both PPC and Conexa SMGW devices could be deemed secure at the current moment of our research.