Fraunhofer FOKUS

FRAUNHOFER INSTITUTE FOR OPEN COMMUNICATION SYSTEMS FOKUS

enyCLS: REMOTE ACCESS TO CONTROLLABLE DEVICES

Contact
Peter Hasse
IT4Energy Center
Phone +49 30 3463-7297
peter.hasse@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

www.it4energy-zentrum.de

</enyCLS>

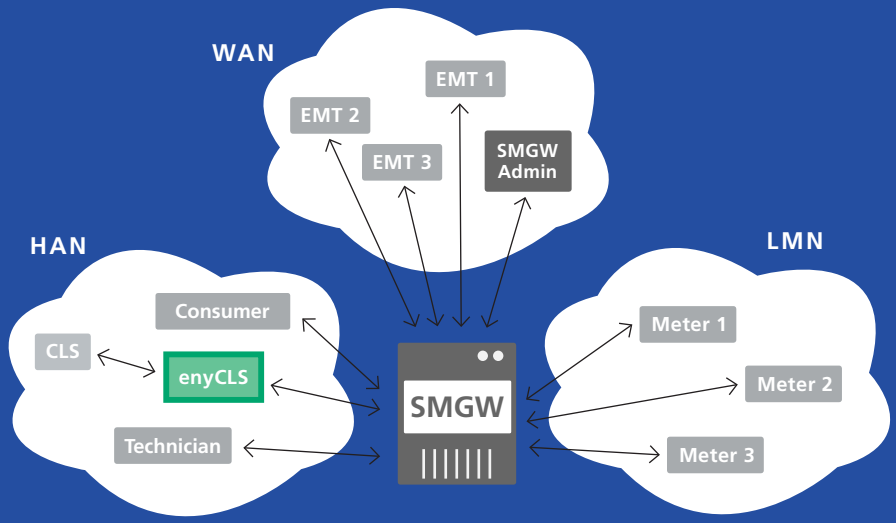
Communication between the different agents in a smart grid, from the energy producer and supplier to the metering system operator and finally the consumer device, is key to balancing the production and the consumption of energy.
The guideline TR-03109 published by the Germany's Federal Office for Information Security (BSI) sets standards for the remote access to controllable devices with respect to communication protocols and security specifications.
In this context, the controllable devices are called »controllable local systems, CLS«, whereas the remote control systems are known as »authorised external market participants, EMT« upon meeting certain functionality requirements, which are implemented by enyCLS.

enyCLS offers a flexible software solution for building a communication tunnel between the control system and the controllable devices, thus enabling the exchange of data between them. The tunnel is:

... **secured** and **trustworthy**, since enyCLS implements the TLS protocol in compliance with the current BSI standards concerning X.509 certificates, encryption algorithms and digital signatures,

... **two-way**, as the communication can be initiated both by the EMT and the CLS,

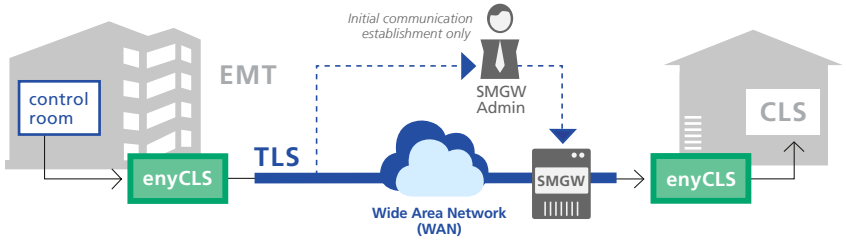
... **application independent**, because any TCP/IP-capable program can be used on both the EMT's and the CLS's side for sending and receiving data that will be encrypted by enyCLS.



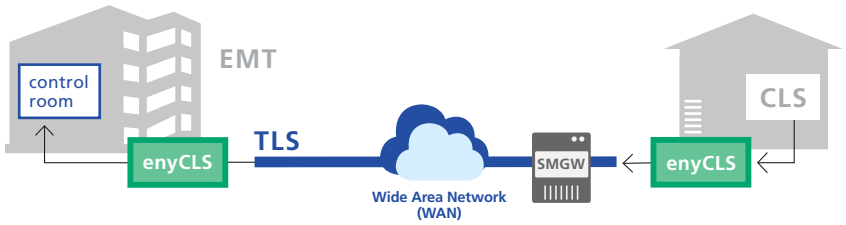
Smart meter gateway infrastructure

Communication scenarios

a) **METER & TRIGGER**



b) **REPORT & NOTIFY**



a) The control room initiates a secure connection to the CLS devices of the customers. This equates to HKS4 defined by BSI. In this way, measurement data can be requested and / or control information can be sent.

b) A consumer's CLS device initiates communication, by using enyCLS on the SMGW a secure connection to an EMT. This equates to HKS3 defined by the BSI. In this way, the CLS device asks or transmits control commands of errors, alarms, and status informations.

Both communication scenarios are suitable for the transfer of measurement and control information, as well as for the transmission of any digital messages.

enyCLS can be used for applications from alarm systems to Smart Home systems in a wide range of scenarios.

Actors

- **EMT:** »Externer Marktteilnehmer«, every agent, excluding the SMGW Admin, with which the SMGW can establish a communication and exchange data.
- **CLS:** »Controllable Local System«, controllable energy consumers and/or producers.[1]
- **SMGW:** »Smart Meter Gateway«, the communication unit in a smart grid.
- **SMGW Admin:** the trustworthy entity that configures, monitors and controls the SMGW.
- **TLS:** »Transport Layer Security«, an encryption protocol for the secure exchange of data in the Internet.

Network

- **WAN =** Wide Area Network
- **HAN =** Home Area Network
- **LMN =** Local Metrological Network

[1] Could be a »prosumer« i. e. producing and consuming energy

Engineering a Connected World