Distributed Controller Communication in Virtual Power Plants Using Smart Meter Gateways

Florian Heimgaertner and Michael Menth
Chair of Communication Networks, University of Tuebingen, Tuebingen, Germany
Email: {florian.heimgaertner,menth}@uni-tuebingen.de

***Abstract*—A virtual power plant (VPP) is a distributed power plant aggregating the capacity of multiple small distributed energy resources (DERs) and acts as a single entity at the energy markets. The VPP needs a secure communication infrastructure to monitor, coordinate, and control the DERs.**

This work describes how a smart meter gateway (SMGW) according to the German regulations can be used to provide a secure communication channel between the central VPP aggregator and distributed DER controllers.

I. Introduction

The increasing share of renewable energy sources and small combined heat and power plants (CHPs) leads to a decentralization of electrical power generation. Together with controllable loads and energy storages, those distributed generators are summarized as distributed energy resources (DERs) [1]. However, most individual DERs are too small to participate in the energy market or are subject to volatility caused by weather-dependent production. A virtual power plant (VPP) is a distributed power plant comprising the aggregated capacity of DERs at multiple locations. The VPP acts like a single entity towards the energy market and can compensate for volatile production within its set of participants by leveraging the capacity of flexible DERs. The central component of a VPP is an aggregator trading at the markets, retrieving measurement data from the DERs, and sending schedules or commands to the DER controllers. For the interactions between the aggregator and the DER controllers, a secure communication channel is required.

To improve grid monitoring and enable time-dependent or dynamic energy tariffs, remote meter reading, and automated billing smart meters are currently being deployed in many countries. In Germany, the proposed advanced metering infrastructure (AMI) requires the separation of the metering component and the communication component. Communication of smart meters to both on-site and remote entities must use a smart meter gateway (SMGW).

A previous work [2] describes the SMGW architecture and presents an experimentation framework with focus on meter data transmission. In this work, we describe how a SMGW can be used for communication of a VPP aggregator and a DER controller.

This work is structured as follows. Section II discusses related work and relevant protocols and standards for the German AMI and VPP communication. Section III describes the concept of a virtual power plant. In Section IV we introduce the basics of the German AMI and the SMGW concept. In Section V we propose using SMGWs as communication infrastructure for VPPs. Section VI concludes the paper.

II. Related Work

The DLMS/COSEM suite is a set of standards for the exchange of energy meter data, comprising of DLMS (device language message specification) [3] as an application layer protocol for communication with metering devices, and COSEM (companion standard for energy metering) [4] as a system for object-oriented modeling of energy metering equipment. DLMS/COSEM uses the object identification system (OBIS) [5] to identify data objects in energy metering systems, and COSEM services enable clients to query specific attributes of objects, assign values to attributes of objects, or execute methods of objects.

SML (smart message language) [6] is a message-oriented protocol for communication with smart meters. The SML application protocol defines SML files consisting of one or multiple SML messages. An SML message can be either a request or a response. Smart meters act as servers, receiving SML files from clients, and processing the contained SML messages in order of reception. Starting with version 1.04, SML supports COSEM services, i.e., the COSEM object model can be used with the SML application protocol. Currently, SML is not widely used outside Germany. However, international use of SML is expected to increase if plans to adopt SML as part of the DLMS/COSEM suite [7] are successful.

M-Bus is a protocol suite for communication with smart meters. M-Bus is defined in the European standard EN 13757 which comprises data model [8], application layer [9], and both wired [10] and wireless [11] specifications for the physical layer. The Open Metering System (OMS) [12], [13] is a smart metering communication architecture based on M-Bus. OMS proposes several modifications to the M-Bus protocols, and adds an optional authentication and fragmentation layer to the M-Bus protocol stack.

The Dutch Smart Meter requirements (DSMR) [14] are a joint specification of the Dutch grid operators. DSMR is based on DLMS/COSEM and M-Bus, and defines a data model for smart meters including corresponding OBIS codes.

VHPready [15] is a requirements specification for DERs to be integrated in a VPP. VHPready uses IEC 61850-7-

2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, June 2018

420 [16], [17] and IEC 60870-5-104 [18] for communication with DERs. In contrast to the communication scheme proposed in this work, VHPready uses a direct control approach without distributed controllers and relies on OpenVPN [19] instead of SMGWs for secure communication channels between DERs and the aggregator.

III. Virtual Power Plants

A VPP consists of distributed generators, energy storage, and controllable loads. Examples for generators are photovoltaic (PV) panels, wind turbines, small hydroelectric systems, fuel cells, or CHPs. Energy storage comprises electrochemical storage (e.g., batteries), mechanical storage (e.g., compressed air tanks or pumped-storage hydro power), and thermal storage. Controllable loads are electric devices with certain flexibility regarding operating times and power input that can be scheduled and controlled (e.g., heat pumps or cooling chambers). Generators, storages, and controllable loads are summarized as DERs. Multiple DERs are coordinated by an aggregator in order to cooperatively act at the energy markets like a single, larger entity. The aggregated capacity of the DERs is comparable to a traditional power plant, leading to the term *virtual power plant*.

Monitoring, management, and optimization systems are required at the aggregator level to achieve this goal. For communication between the aggregator and the DERs a reliable and secure communication channel is needed.

While medium-sized distributed generators such as CHPs or wind turbines are usually directly connected to an aggregator, small generators, controllable loads, and storage units are often available at the same site and need local coordination. For local coordination, DER controllers can be installed on-site to concentrate the communication between the aggregator and multiple DERs.

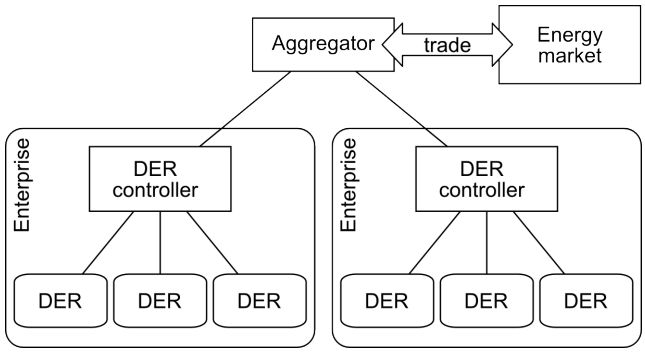

Fig. 1: Hierarchical VPP architecture with distributed controllers.

The introduction of distributed controllers leads to a hierarchical VPP architecture as depicted in Figure 1 with an aggregator at the top level, controllers at the second level and DERs at the third level.

Business models for VPPs include selling energy at the spot market or providing ancillary services for the electrical power grids like operating reserve.

Microgrids also consist of DERs connected by communication infrastructure and are coordinated by management and control systems. The concept of a microgrid is similar to that of a VPP. However, microgrids are more focused on the power grid side and require separate distribution grids for use cases like islanding operation (i.e., operation of a local distribution grid temporarily disconnected from the main grid).

IV. Smart Meter Gateways

The main advantage of smart meters over legacy electromechanical meters is the possibility of remote meter reading, dynamic tariffs, and automated billing. To implement those features, smart meters need communication capabilities in order to connect to energy service providers over wide area networks.

Smart meters are subject to gauging and calibration regulations and need to be inalterable and tamper-proof. In contrast, communication devices may require reconfiguration or security updates while they are in the field. To resolve this conflict and keep the smart meters minimal, the proposed German AMI [20], [21] mandates the separation of metering components and communication components. SMGWs are the central communication components in the German AMI. SMGWs are responsible for gathering of metering data from smart meters and providing a unified interface for metering data retrieval to interested and legitimate external market participants. The smart meters only provide minimal communication capabilities to connect to a SMGW. Additionally, a SMGW further allows to install smart meters of different vendors in the same households, connecting them to the same SMGW. We briefly discuss the system boundaries, functionalities, communication, and security of a SMGW-based smart metering architecture as defined in [20], [21].

A. Connected Networks

In general, the SMGW mediates between three networks, as shown in Figure 2: the local metrological network (LMN), the home area network (HAN), and the wide area network (WAN). The LMN connects smart meters to the SMGW only. The HAN connects end consumers, service technicians, and controllable local systems (CLSs) to the SMGW, e.g., electric vehicles, photo-voltaic panels, remote-controllable heating, and air conditioning. The WAN connects SMGW administrators (GWA) and external market participants (EMPs) to the SMGW, e.g., distribution grid operators, metering point operators, and suppliers of electric energy.

B. Functionalities and Communication

The functionalities and the used communication protocols of SMGWs can be differentiated by the networks they mediate between.

In the LMN, SMGWs are responsible for gathering metering data from smart meters according to metering profiles, time-stamping the measurements based on an externally synchronized time source, tariffing, and finally storing the time-stamped, tariffed metering data for further dissemination

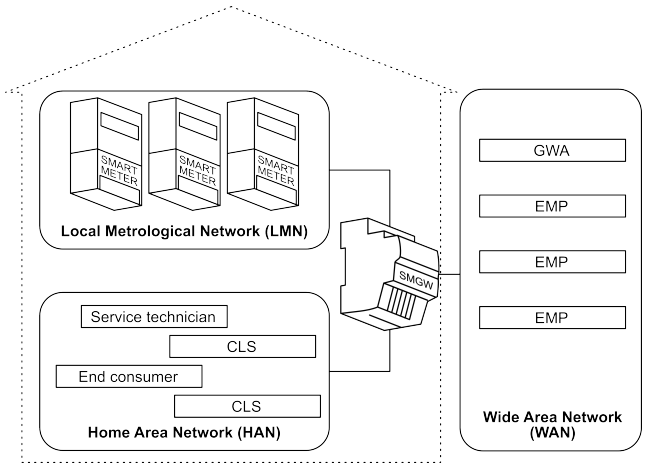

Fig. 2: Networks connected to a SMGW according to [21]. The SMGW mediates between LMN, HAN, and WAN.

to EMPs. SMGWs support bidirectional and unidirectional communication with smart meters. Bidirectional communication involves interactive communication between SMGWs and smart meters to poll for metering data or to manage smart meters. Unidirectional communication stands for unsolicited metering data dissemination from smart meters to SMGWs. Generally, COSEM [4] with OBIS [5] codes are used as data model between smart meters and SMGWs. Depending on the underlying physical layer, M-Bus [8]–[11] or SML [6] is used as transport protocol.

In the HAN, SMGWs provide read-only access to their internally stored metering data and status messages to end consumers. SMGWs can support several end consumers facilitating multi-client operation, e.g., in an environment involving many smart meters and many households. Service technicians must only access status messages of SMGWs. SMGWs relay control messages between CLSs and EMPs as configured by the GWA. [21] does not specify protocols between SMGWs and potential HAN communication partners but security mechanisms to be used, e.g., secure transport layer communication, and mandatory authentication of clients against the SMGW. Essentially, any IP-based protocol may be used between SMGWs and HAN entities, e.g., end consumers or service technicians.

In the WAN, SMGWs are responsible for forwarding their internally stored metering data to interested and legitimate EMPs based on communication profiles. SMGWs must not accept connections from the WAN for security reasons but a wake-up service facilitates remote SMGW administration. When SMGWs receive specific control packets from the WAN, they contact an external GWA for maintenance, e.g., for firmware updates, changes in the communication profiles, time synchronization, or access to status messages. WAN communication is based on RESTful web services as defined in [21], and SMGWs act as RESTful web service clients because they must not accept connections from the WAN. EMPs must provide the server side of a RESTful web service according to the interface definitions in [21], [22]. As for LMN communication, COSEM with OBIS codes are used as data model between SMGWs and EMPs but XML and cryptographic message syntax (CMS) [23] are used as transport protocol on top of REST. Time synchronization of SMGWs is handled over the network time protocol (NTP).

C. Security

The BSI SMGW protection profile (SMGW-PP) [24] requires all LMN, HAN and WAN communication to be secured by transport layer security (TLS) [25] in combination with a public-key infrastructure [26], [27]. WAN communication is further protected by CMS between SMGWs and EMPs. SMGWs are equipped with a security module which provides cryptographic functions, e.g., generation and secure storage of encryption keys, and verification of digital certificates. The security module is realized as a smart card. Further information on the security module and its requirements can be found in [28]–[30].

V. VPP Communication using SMGWs

Communication protocols, technologies, and formats between controllers and DER are determined by the controlled devices. Relevant technologies in this area are Modbus-TCP [31], [32], IEC 60870-5-104 [18], and direct control over analog ar digital I/O. In the following, we focus on the communication between aggregators and controllers and show, how SMGWs can be used to provide a communication channel.

The technical guideline TR-03109 [20] defines three separate communication networks connected to a SMGW. The LMN connects smart meters to the SMGW. The WAN allows access by EMPs and GWAs. The HAN contains CLSs and interfaces for the end user. The technical guidelines assume CLSs to be individual DERs. For a hierarchical VPP implementation as shown in Section III we propose that the DER controller acts as a CLS. The structure is shown in Figure 3. The DER controllers are CLSs in the HANs of the VPP participants. The aggregator is an EMP located in the WAN.

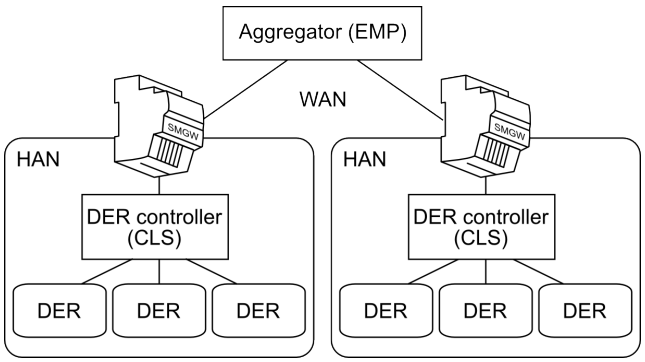

Fig. 3: Communication between aggregator and DER controllers via SMGWs in a hierarchical VPP.

The requirements specification for the interoperability of SMGWs (BSI TR-03109-1) [21] specifies several use cases

and communication scenarios. HAN use case 3 (HAF3)[1] describes a proxy feature where the SMGW provides a transparent communication channel between CLSs and EMPs. HAN communication scenarios 3–5 (HKS3–5) of [21] specify different variants, how this transparent tunnel is established.

A. Tunnel Initiated by CLS

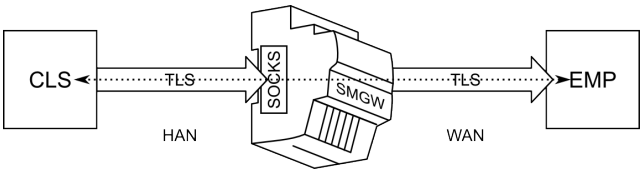

Fig. 4: HAN Communication Scenario 3 (HKS3): transparent tunnel initiated by CLS.

HAN communication scenario 3 (HKS3) describes a transparent tunnel between CLS and EMP via SMGW initiated by the CLS. The scenario is shown in Figure 4. The CLS initiates a TLS [25] secured connection to the SMGW and the SMGW initiates a TLS connection to the EMP. The SMGW forwards data received from the CLS to the EMP and vice versa.

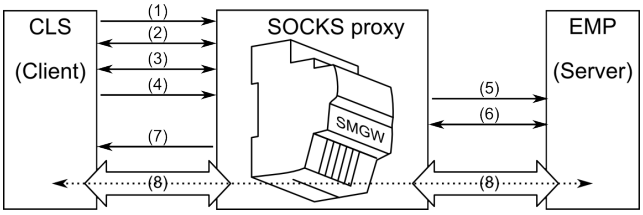

Fig. 5: Signaling for the initiation of the tunnel by the CLS using the SOCKS protocol.

The mechanism to enable the initiation of the tunnel by a CLS is implemented using the SOCKS [33] protocol. A CLS can only connect to destination EMPs that have been previously permitted by the GWA. In HKS3, the CLS is a SOCKSv5 client, the SMGW is a SOCKSv5 proxy server, and the EMP is a TLS server. Figure 5 depicts the signaling to establish the tunnel. In step (1) the CLS connects to the SOCKS server of the SMGW. The SMGW and the CLS negotiate TLS as SOCKS authentication method in step (2). After the TLS handshake (3) is completed, the CLS issues a connect request (4) for the destination address of the EMP. If the EMP address is a permitted destination, the SMGW connects to the EMP server (5). After the TLS handshake (6) between the SMGW and the EMP server, the SMGW sends the SOCKS response to the CLS (7) and the tunnel between the CLS and the EMP is established (8).

B. Tunnel Initiated by EMP

HAN communication scenario 4 (HKS4) describes the transparent tunnel between CLS and EMP via the SMGW initiated by the EMP. For security reasons, the SMGW does not accept incoming connections from the WAN [24]. The only exception from this policy is the wake-up service [21] that allows the GWA to send a notification packet to the SMGW from the WAN. The signaling is depicted in Figure 6. To initiate the tunnel, the EMP contacts the GWA and request to wake up the SMGW (1). Upon reception and verification of a wake-up packet (2), the SMGW establishes a connection to the GWA (3) and awaits commands. The GWA instructs the SMGW to open TLS connections to the CLS and the EMP (4). In HKS4, both the CLS and the EMP are TLS servers while the SMGW is a TLS client.

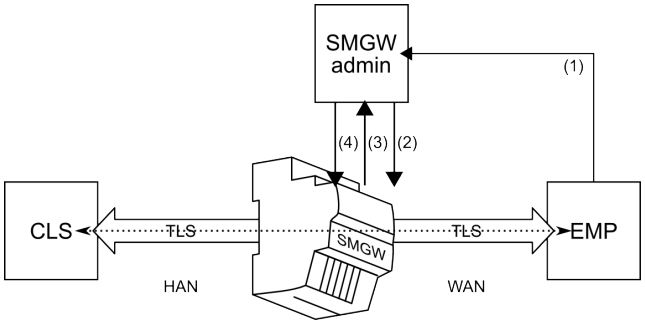

Fig. 6: HAN Communication Scenario 4 (HKS4): Transparent tunnel initiated by EMP.

C. Tunnel Triggered by Event or Timer

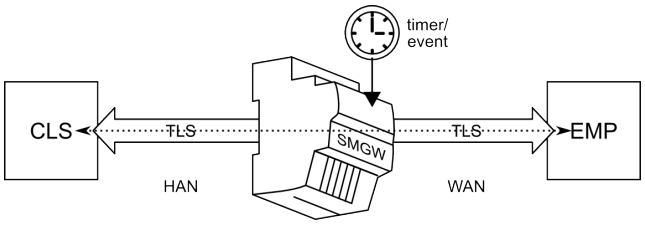

Fig. 7: HAN Communication Scenario 5 (HKS5): Transparent tunnel triggered by event or timer.

HAN communication scenario 5 (HKS5) describes the transparent tunnel between CLS and EMP via SMGW triggered by a timer or event. The scenario is shown in Figure 7. If the timer is elapsed or a configured event occurs, the SMGW opens TLS connections to the CLS and the EMP. The timers or events must be configured by the GWA. In HKS5, both the CLS and the EMP are TLS servers while the SMGW is a TLS client.

D. Communication Security

For authentication during the TLS handshake, the SMGW holds separate X.509 certificates for the HAN and the WAN. The private keys for the certificates are stored in the hardware security module [24], [30] of the SMGW. The CLSs, the EMPs and the GWA also have TLS X.509 certificates.

While the CLS certificates and the HAN certificate of the SMGW may be self-signed or issued by a vendor certification

[1]See Table II for information about abbreviations derived from German terminology.

authority (CA), the EMP certificates and the WAN certificate of the SMGW must be part of the German smart metering public key infrastructure (SM-PKI) [34]. The structure of the PKIs involved in the German AMI is depicted in Figure 8. The trust anchor of the SM-PKI is a government-operated root CA. X.509 certificates for SMGWs, GWAs, and EMPs are issued by licensed sub-CAs of the SM-PKI. The CA certificates of the sub-CAs are signed by the SM-PKI root CA.

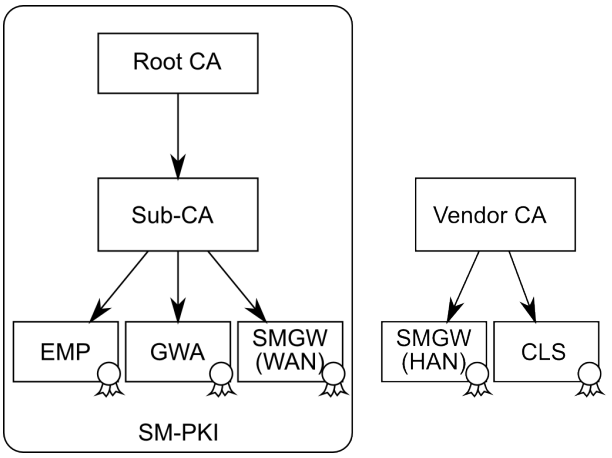

Fig. 8: Public key infrastructures and certificates for the German AMI.

In addition to the X.509 certificates for TLS, the AMI pariticpants may have separate X.509 certificates for content data encryption and digital signatures. While the content data encryption certificates are not relevant for the scenarios illustrated in this work, digital signature certificates are used for signing the wake-up message sent by the GWA to the SMGW in HKS4.

The communication relationships between CLSs and EMPs are configured in proxy communication profiles (PCP) by the GWA. A PCP contains the addresses of both end points and the associated X.509 TLS certificates. In HKS3–5 the SMGW authenticates both the CLS and the EMP during the TLS handshake using the certificates stored in the corresponding PCP. TLS communication involving the SMGW must use version 1.2 [25] of the TLS protocol. BSI TR-03116-3 [29] mandates the use of the following cryptographic primitives. The ephemeral elliptic-curve Diffie-Hellman (ECDHE) [35] method is used for key exchange, the elliptic-curve digital signature algorithm (ECDSA) [35] is used for authentication, the advanced encryption standard (AES) block cipher in cipher block chaining (CBC) or galois counter mode (GCM) is used for encryption, and the secure hash algorithm (SHA) variants SHA256 or SHA384 are used as cryptographic hash functions.

The use of TLS does not provide actual end-to-end encryption in any of the proposed communication scenarios for HAF3, as both TLS connections are terminated at the SMGW. Integrity and confidentiality of the communication between CLS and EMP are protected against attackers controlling the network infrastructure of either the HAN or the WAN. However, an attacker controlling the SMGW would be able to read or modify transmitted information. If end-to-end confidentiality and authenticity is required for the communication, additional security mechanisms need to be applied within the tunnel.

E. Scenario Recommendation

Table I lists the role of the GWA in each of the three communication scenarios. The GWAs configure the permitted WAN communication endpoints in HKS3, they instruct the SMGWs on behalf of the EMP to establish the connections in HKS4, and in HKS5 they configure the rules that determine how to act upon events or elapsed timers. While HKS3 and HKS5 require the cooperation of the GWA only once, HKS4 involves the SGMW-admin each time a connection is to be established.

TABLE I: Role of the SMGW Administrator (GWA).

Scenario	GWA responsibility	Frequency
HKS3	Setup of PCP (permitted destination)	once
HKS4	Setup of PCP	once
	Wake up SMGW and initiate tunnel	per-connection
HKS5	Setup of PCP (timers or events)	once

To reduce dependencies on external service providers such as the GWAs and to avoid the additional costs, we propose to prefer HKS3 and HKS5 over HKS4. Both HKS3 and HKS5 only involve the GWA for the configuration of the PCP. However, the configuration required for HKS5 is more complex and the PCP can be expected to change more often than for HKS3. Therefore, we propose a communication scheme according to HKS3 with the communication tunnel initiated by the CLS, i.e., the DER controller.

After a connection is established, both the CLS and the EMP can initiate the transfer of data. Therefore, communication according to HKS3 can also be used if the interaction at the application layer is supposed to be initiated by the EMP. For this purpose, a CLS can be configured to initiate a tunnel and wait for actions of the EMP. However, the CLS needs to re-establish the tunnel periodically, as BSI TR-03116-3 [29] does not permit TLS sessions to take longer than 48 hours.

VI. Conclusion

Virtual power plants work by coordinating the operation of multiple DERs. For monitoring and control of devices distributed over different sites, a secure and reliable communication channel is required. For Germany, BSI TR-03109 defines an AMI based on SMGWs. In this paper, we identified options how to connect distributed controllers to the aggregator of a VPP using SMGWs. We illustrated the signaling and the security properties and recommended one of the scenarios proposed in BSI TR-03109 for the communication.

Acknowledgment

The research leading to these results has received funding from the German Federal Ministry for Economic Affairs and Energy under the ZIM programme (Zentrales Innovationsprogramm Mittelstand), grant no. 16KN039521 and from

the Ministry of the Environment, Climate Protection and the Energy Sector Baden-Württemberg within the demonstration project "Virtuelles Kraftwerk Neckar-Alb" under the programme "Smart Grids und Speicher Baden-Württemberg" grant no. BWSGD 15012. The authors alone are responsible for the content of this paper.

The authors thank Michael Hoefling, Andreas Stockmayer, and Daniel Merling for valuable feedback.

TERMINOLOGY

Table II lists and explains the abbreviations used within this paper. Additionally, for abbreviations derived from German terminology where the letters do not match the English description the German meaning is given in parentheses.

TABLE II: List of Abbreviations.

Abbreviation	Description
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
BSI	German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CA	Certification Authority
CBC	Cipher Block Chaining
CHP	Combined Heat and Power Plant
CLS	Controllable Local System
CMS	Cryptographic Message Syntax
DER	Distributed Energy Resource
ECDHE	Ephemeral Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EMP	External Market Participant
GCM	Galois Counter Mode
GWA	Smart Meter Gateway Administrator
HAF	HAN Use Case (HAN-Anwendungsfall)
HAN	Home Area Network
HKS	HAN Communication Scenario (HAN-Kommunikationszenario)
LMN	Local Metrological Network
OBIS	Object Identification System
PCP	Proxy Communication Profile
PKI	Public Key Infrastructure
SHA	Secure Hash Algorithm
SM-PKI	Smart Metering PKI
SMGW	Smart Meter Gateway
TLS	Transport Layer Security
TR	Technical Guideline (Technische Richtlinie)
VPP	Virtual Power Plant
WAN	Wide Area Network

REFERENCES

[1] C. Marnay, S. Chatzivasileiadis, C. Abbey, R. Iravani, G. Joos, P. Lombardi, P. Mancarella, and J. von Appen, "Microgrid Evolution Roadmap," in *International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, 2015.

[2] M. Hoefling, F. Heimgaertner, D. Fuchs, and M. Menth, "jOSEF: A Java-Based Open-Source Smart Meter Gateway Experimentation Framework," in *D-A-CH Conference on Energy Informatics*, Karlsruhe, Germany, Nov. 2015.

[3] International Electrotechnical Comission, "Electricity Metering Data Exchange - The DLMS/COSEM Suite - Part 5-3: DLMS/COSEM Application Layer," IEC 62056-5-3 ed3.0, 2017.

[4] ——, "Electricity Metering Data Exchange - The DLMS/COSEM Suite - Part 6-2: COSEM Interface Classes," IEC 62056-6-2 ed3.0, 2017.

[5] ——, "Electricity Metering Data Exchange - The DLMS/COSEM Suite - Part 6-1: Object Identification System (OBIS) ," IEC 62056-6-1 ed3.0, 2017.

[6] German Federal Office for Information Security (BSI), "BSI TR-03109-1 Anlage IV: Feinspezifikation Drahtgebundene LMN-Schnittstelle, Teil b: SML - Smart Message Language," SML Version 1.04, 2013.

[7] International Electrotechnical Comission, "Electricity Metering Data Exchange - Part 5-3-8 Smart Message Language SML," IEC 62056-5-3-8 (future standard).

[8] European Committee for Standardization, "Communication Systems for and Remote Reading of Meters - Part 1: Data Exchange," EN 13757-1:2015-01, 2015.

[9] ——, "Communication Systems for and Remote Reading of Meters - Part 4: Wireless Meter Readout," EN 13757-4:2014-02, 2014.

[10] ——, "Communication Systems for and Remote Reading of Meters - Part 2: Physical and Link Layer," EN 13757-2:2004, 2004.

[11] ——, "Communication Systems for and Remote Reading of Meters - Part 3: Dedicated Application Layer," EN 13757-3:2013-08, 2013.

[12] OMS Group, "Open Metering System Specification, Volume 1: General Part," OMS Spec Vol1 1.4.0, 2011.

[13] ——, "Open Metering System Specification, Volume 2: Primary Communication, Version 4.0.2," OMS Spec Vol2 4.0.2, 2014.

[14] Netbeheer Nederland, "Dutch Smart Meter Requirements: P1 Companion Standard," DSMR Version 5.0, 2014.

[15] Industrieforum VHPready, "VHPready Anforderungsspezifikationen 3.0," http://www.vhpready.de/, 2012.

[16] IEC, "IEC 61850-7-420: Communication Networks and Systems for Power Utility Automation - Distributed Energy Resources Logical Nodes," 2009.

[17] N. Etherden, V. Vyatkin, and M. Bollen, "Virtual Power Plant for Grid Services using IEC 61850," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 437–447, 2016.

[18] IEC, "IEC 60870-5-104: Network Access for IEC 60870-5-101 Using Standard Transport Profiles," 2000.

[19] J. Yonan, "OpenVPN – An Open Source SSL VPN Solution," http://openvpn.net, 2008.

[20] German Federal Office for Information Security (BSI), "Technische Richtlinie BSI TR-03109," 2013.

[21] ——, "Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Technische Richtlinie BSI TR-03109-1, Version 1.0," 2013.

[22] ——, "BSI TR-03109-1 Anlage II: COSEM/HTTP Webservices," 2013.

[23] ——, "BSI TR-03109-1 Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur," 2013.

[24] ——, "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)," BSI SMGW-PP 1.3, 2014.

[25] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 https://www.ietf.org/rfc/rfc5246.txt, Aug. 2008.

[26] German Federal Office for Information Security (BSI), "Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Technische Richtlinie BSI TR-03109-3, Version 1.1," 2014.

[27] ——, "Public Key Infrastruktur für Smart Meter Gateways, Technische Richtlinie BSI TR-03109-4, Version 1.0," 2013.

[28] ——, "Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Technische Richtlinie BSI TR-03109-2, Version 1.1," 2014.

[29] ——, "Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme, Technische Richtlinie BSI TR-03116-3," 2017.

[30] ——, "Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.02," BSI SecMod-PP 1.02, 2013.

[31] Modbus IDA, "Modbus Application Protocol Specification v1.1b3," 2012.

[32] ——, "Modbus Messaging on TCP/IP Implementation Guide V1.0b," 2006.

[33] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, "SOCKS Protocol Version 5," RFC 1928 https://tools.ietf.org/rfc/rfc1928.txt, Mar. 1996.

[34] German Federal Office for Information Security (BSI), "Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, Technische Richtlinie BSI TR-03109-4, Version 1.2.1," 2017.

[35] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)," RFC 4492 https://www.ietf.org/rfc/rfc4492.txt, May 2006.