Security guide for Industrial Protocols
Smart Grid

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
incibe cert_

May 2020

INCIBE-CERT_GUIDE_PROTOCOLS_SMART_GRID_2017_v2

Contents

FIGURES INDEX

TABLES INDEX

1. About this guide

Following the line of the study "*Protocols and network security in ICS infrastructure*"[1], published by INCIBE, where a vision of the most representative protocols in control systems is offered, this document intends to take a deeper look at the protocols used in smart grids.

This study, of a technical nature, is focused on smart grid communications, and is intended to offer a vision of the most used protocols in Spain and Europe showing their functionalities, the security measures they offer and the problems they face. Similarly, a series of recommendations are provided in each of them, for the purpose of improving the security of the facilities that have implemented them.

[1] https://www.incibe-cert.es/en/publications/guides/ics-network-security

2. Introduction and current situation

For some years, the electricity grid has undergone a great transformation promoted, above all, at European level through the "20-20-20 Objectives"[2]. The basis of the modification of the electrical grid arises in the communication COM (2006) 786 "On a European Programme for Critical Infrastructure Protection"[3] of the European Commission, where the principal aspects of the European Programme for Critical Infrastructures Protection (EPCIP) were defined; and most importantly with the publication by the European Commission of communication COM (2011) 202, "Smart Grids: from Innovation to Deployment"[4].

This has also affected communications, creating new networks and new specific protocols for this sector. Certain tasks, now in demand, require the use of bidirectional communications between the final section of electrical distribution, also called the last mile, which covers the section from the transformation centres to the meter located in the customer's house/building; and the control centres, to pass on information to the final customer or to manage the production of, and demand for, energy, as can be seen in the scheme in Figure 1.

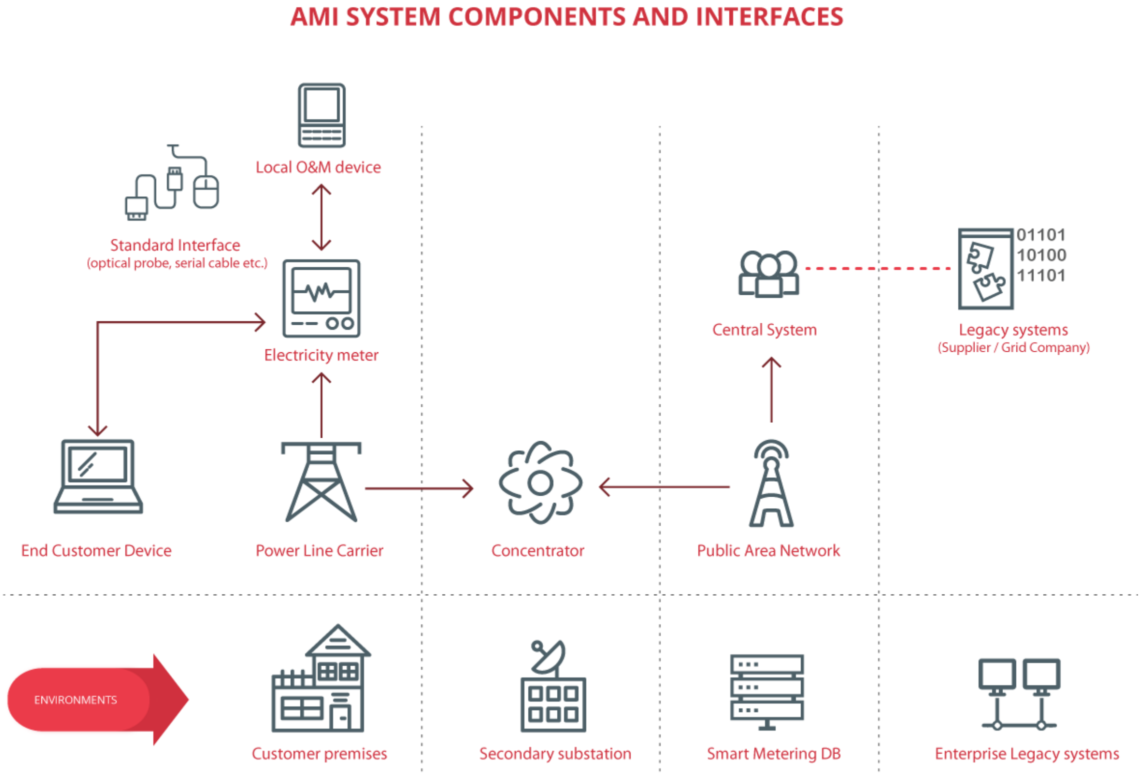

Figure 1 Main components of Advanced Measure Infrastructure (AMI) Source: METERS AND MORE

[2] http://ec.europa.eu/clima/policies/strategies/2020/index_es.htm

[3] http://www.iserd.org.il/_Uploads/dbsAttachedFiles/com2006_0786en01.pdf

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

3. Protocols and points of analysis

3.1. Protocols under analyse

Thanks to the unification and standardisation established between energy distributors, manufacturers and developers, the existence of protocols related to smart grids is not as widespread as in other areas of industry. From among protocols arising from this unification and standardisation, those used most commonly in Spain, along with those most widely used across Europe, are analysed here.

The protocols selected are the following:

- PRIME
- Meters and More
- G3-PLC
- OSGP
- DLMS/COSEM
- IEEE 1901

3.2. Layers of the protocols

The industrial network protocols are, for the most part, new generation, implying a separation of functions in their specification which is equivalent to the levels of the OSI scheme, unlike the old control system protocols which had diffuse borders.

Throughout this study, reference shall be made, on various occasions, to the OSI layer model to explain those each protocol interacts with. Protocols used for distribution control and electrical consumption usually have more than one definition of layer 1, or the physical layer, due to the variety of communications available in the devices.

3.3. Security elements and recommendations

For each of the protocols selected, there is a description of same, indicating their strengths and weaknesses in terms of security. To finish, a series of recommendations are provided to apply to use the best security features for each use of the protocol.

4. Analysis of communication protocols in smart grids

4.1. PRIME

4.1.1. Description

PRIME (PoweRline Intelligent Metering Evolution) is a new generation protocol controlled by the PRIME Alliance [5], which implements the first two levels of the OSI model, the physical layer and the link layer.

On the physical level, PRIME uses PLC (Power Line Communications) technology[6], originally in the CENELEN-A (3-95 KHz) but extended to 500 KHz in the latest standard version (PRIME Version 1.4[7]), using an OFDM (Orthogonal Frequency-division Multiplexing) modulation[8].

On the link level, it defines a medium access layer where there is a tree network structure with two different types of nodes for the network, as can be seen in Figure 2:

- Base node: Element corresponding to the root of the tree and acting as the communication master. There is only one base node in each subnet. Initially, this comprises the entire subnet until different service nodes are associated with same.
- Service node: Element found initially in disconnected state and which must go through a registration process to join the network. Service nodes have two functions: to maintain the connection in the subnet for the application layer and to act as the connection's router for the other service node data. There are three different states for a service node:
    - Disconnected: The node is not connected to the subnet.
    - Terminal: The node is connected to the subnet but is not performing routing tasks. It acts as a leaf node of the tree.
    - Switch: The service node is connected to the network and is also performing routing functions of the subnet. It acts as a branch node of the tree.

[5] http://www.prime-alliance.org/

[6] http://es.wikipedia.org/wiki/Power_Line_Communications

[7] http://www.prime-alliance.org/wp-content/uploads/2014/10/PRIME-Spec_v1.4-20141031.pdf

[8] https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiple_access

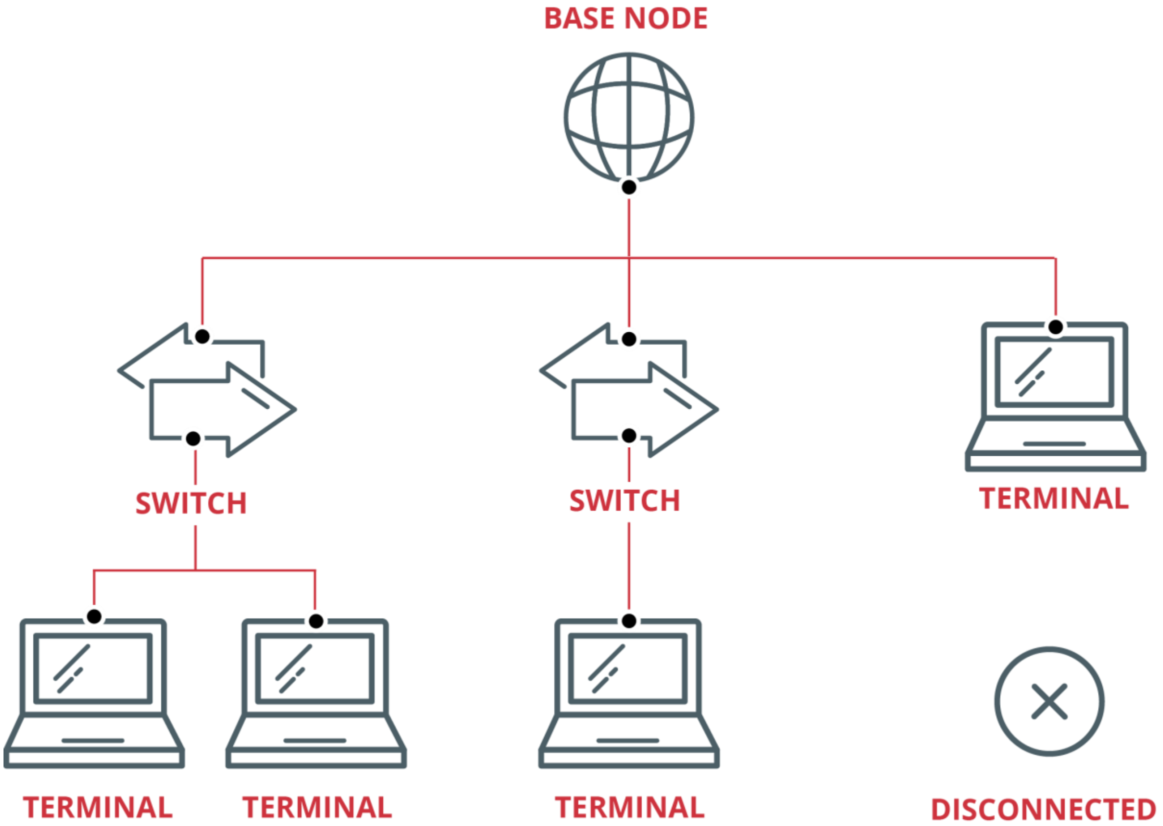

Figure 2. PRIME topology

PRIME is mainly used in Europe, with Spain being one of the countries with the most widespread implementation thanks to the companies Iberdrola (principal founder and driving force behind the alliance) and Gas Natural Fenosa, although its use has also been expanded to other parts of the world, as can be seen in Figure 3.

Figure 3. Area of use of the PRIME protocol Source: PRIME ALLIANCE

The launch of devices with PRIME technology exceeds 10 million devices around the world.

4.1.2. Security

In terms of security, PRIME defines 3 different profiles, at the MAC layer or level 2 layer:

- Security profile 0: does not provide encryption and protection is relegated to the security level provided by higher layers.

- Security profiles 1 and 2: Provide encryption. Profile 2 appears with the specification 1.4 of the protocol and is differentiated from profile 1 in that it encrypts more types of packets, basing itself on cryptographic primitives and using AES128. The advantages provided by the encryption are:
  - Confidentiality, authenticity and integrity of packets guaranteed for the use of the encryption algorithm at the link layer level.
  - Authentication guaranteed because each node possesses its own unique key, known only to the node itself and the base node, and which is established in the manufacturing of the device.
  - Prevention of repetition attacks through the use of a 4-byte field for the packet counter.

The security mechanisms proposed in the security profiles do not protect against media attacks (time attacks, electrical attacks or electromagnetic attacks, noise in the channel, etc.).

4.1.3. Security recommendations

PRIME communications are accessible to any user with access to the electrical grid in which the devices this protocol uses are to be found.

To protect the communications using PRIME protocol it is advisable to use the security profile 1 or 2 as these provide encryption. It must be borne in mind that PRIME only acts on the lower levels of the OSI model and the protocol used on higher level may provide security for messages, making it possible in such cases to use profile 0, assuming that the PRIME communication can be observed, with encryption not applied.

Security profile 0 should only be used in fully controlled environments and where there is no possibility of unauthorised access; or where the data transmitted is for public use and, therefore, not critical to the system.

4.2. Meters and More

4.2.1. Description

Meters and More[9] is the evolution of the proprietary teleprocessing protocol of the Italian energy company ENEL, which has been used in Spain in light of its purchase of the company ENDESA. At present, an alliance has been created to promote the open use of the protocol with other competitors and manufacturers.

Meters and More protocol covers the full stack of the OSI model, from the physical level to the application level, allowing for use of different transmission media:

- PLC profile: For communication between smart meters and concentrators.
- IP profile: For communications through public grids between the central system and the concentrator.
- IEC62056-21[10] Profile. For local access through the optical communications port.

[9] http://www.metersandmore.com/

[10] http://en.wikipedia.org/wiki/IEC_62056

- DLMS/COSEM Profile (see section 4.5). For PLC communications using an exchange of COSEM objects such as an alternative to the PLC profile.

Figure 4 displays the diagram of layers in each of the variations of the protocol.

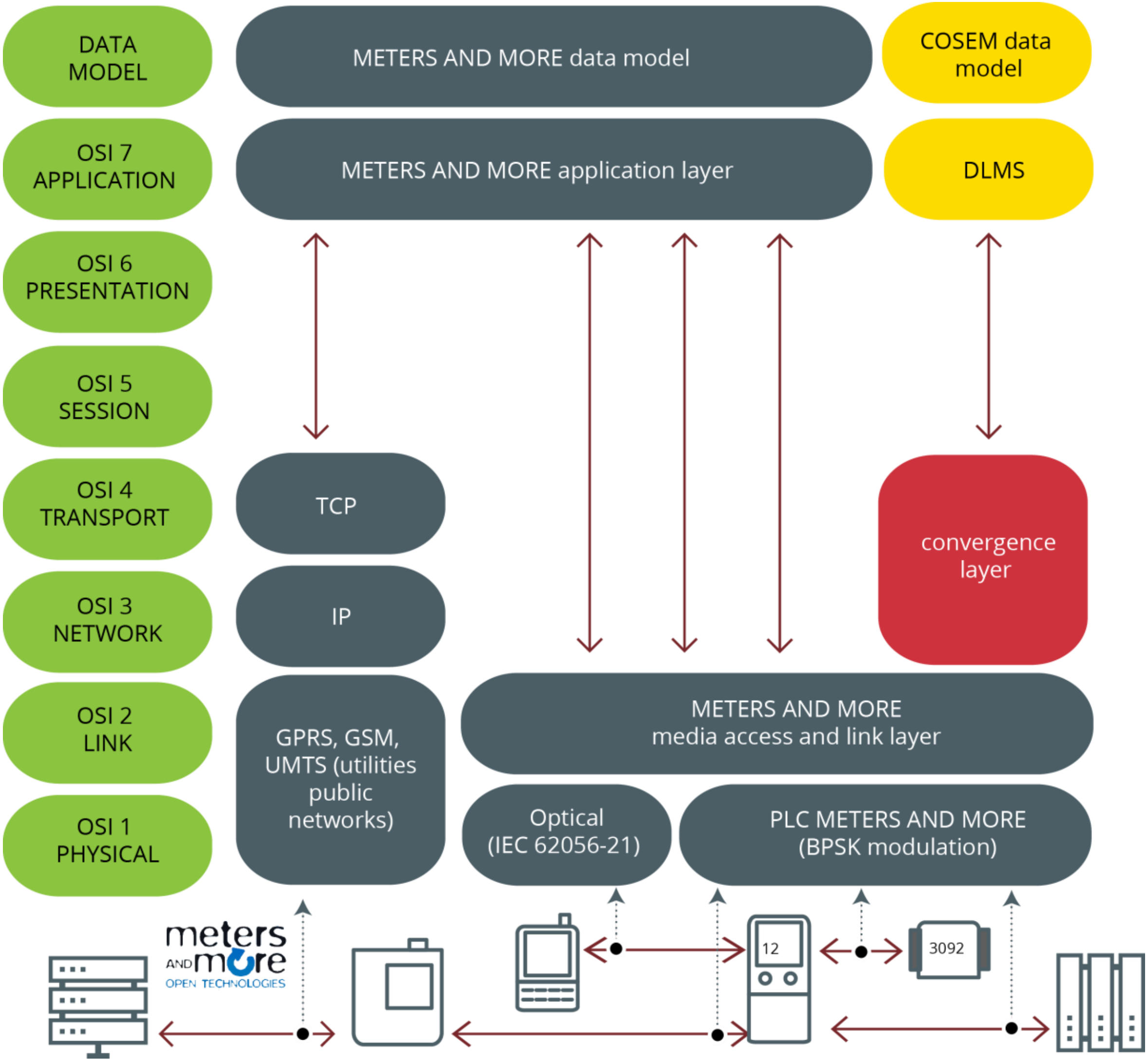

Figure 4. Meters and More architecture. Source: Enginyers Industrials de Catalunya

In Italy there are already more than 35 million devices deployed using this protocol and it is expected that in Spain another 15 million will be installed by 2018, within the ENEL – ENDESA environment alone.

4.2.2. Security

On the security level, *Meters and More* protocol presents the following features within the media access layer or layer 2 of the OSI model:

- Encrypted through 128 bit AES keys.
- Authentication based on symmetric keys.
- Protection against retransmission attacks.
- Checking of message integrity.
- Individual keys for each meter, with access control (reading/writing).

- End-to-End protection.

Messages are encrypted and authenticated through the same key.

4.2.3. Security recommendations

The *Meters and More* protocol incorporates security features into its design, meaning that its use is advisable provided those features are used appropriately.

Focussing on the joint use of Meters and More with DLMS/COSEM, all security should not be left to this second protocol, and security measures of *Meters and More* itself ought to be used also.

In mixed environments where the protocols commented on are used jointly, it is recommended that all the security measures of *Meters and More* are applied to those additional security features provided by DLMS/COSEM (see section 4.5.2 and section 4.5.3).

4.3. G3-PLC

4.3.1. Description

G3-PLC[11] is a standard international open protocol developed specifically for smart grids by Sagem [12], ERDF[13] and Maxim[14], which operates at low frequency, below 500 kHz, promoting the interoperability between 10 kHz and 490 kHz in their communication. It supports different modulations of OFDM and consists of a highly reliable protocol with bidirectional communication. The G3-PLC specification includes the physical and link layers (MAC), where it is supported on OFDM, and a 6LoWPAN[15] adaptation layer to transmit IPv6 packets through the network. These characteristics ensure that this protocol is designed for infrastructures with multiple nodes on a large scale.

The protocol is promoted by the French distribution system operator (ERDF).

The following are some of the features of this protocol:

- Robustness and a wide range of communication frequencies that provide a great advantage when it comes to installing smart devices that send data to the concentrators.
- Design that allows for end-to-end communication through IPv6.
- It uses the bands defined by CENELEC[16], FCC[17] and ARIB[18]:

[11] http://www.g3-plc.com/

[12] http://www.sagem.com/

[13] http://www.erdf.fr/

[14] http://www.maximintegrated.com/

[15] https://en.wikipedia.org/wiki/6LoWPAN

[16] http://www.cenelec.eu/

[17] https://www.fcc.gov/

[18] http://www.arib.or.jp/english/index.html

- Section 15 of the FCC rules establishes that the frequency of the band for PLC in North America must be between 10 and 490 kHz.
- ARIB establishes that the frequency for the PLC band in Asia must be between 10 and 450 kHz.
- CENELEC EN50065-1 defines the range for the low-frequency bands for PLC in Europe:

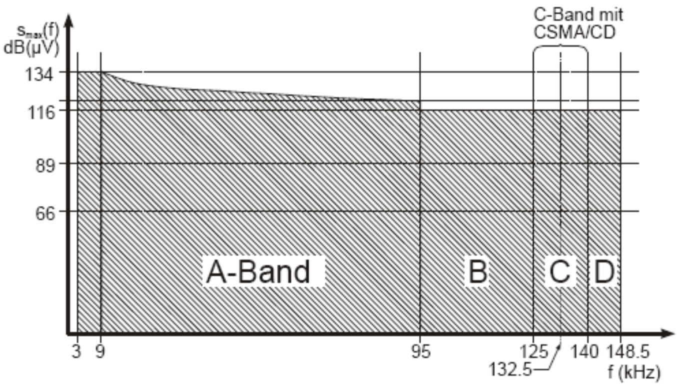

Figure 5. Frequency bands defined by CENELEC. Source: [ResearchGate]

  - A Band (3-95 kHz): The frequencies of this band are only used for the monitoring or control of the low voltage section of the distribution network, including energy consumption data of connected equipment and facilities.
  - B Band (95-125 kHz): Can be used for all types of applications.
  - C Band (125-140 kHz): For domestic network systems.
  - D Band (140-148.5 kHz): specifically for alarms and security systems.

- This is new technology, but committed to the final adjustments and objectives which mark the 20-20-20 Objectives for smart grids.

In order to understand the functioning of the G3-PLC protocol in depth, it is necessary to see a detailed description of the layers where it is present.

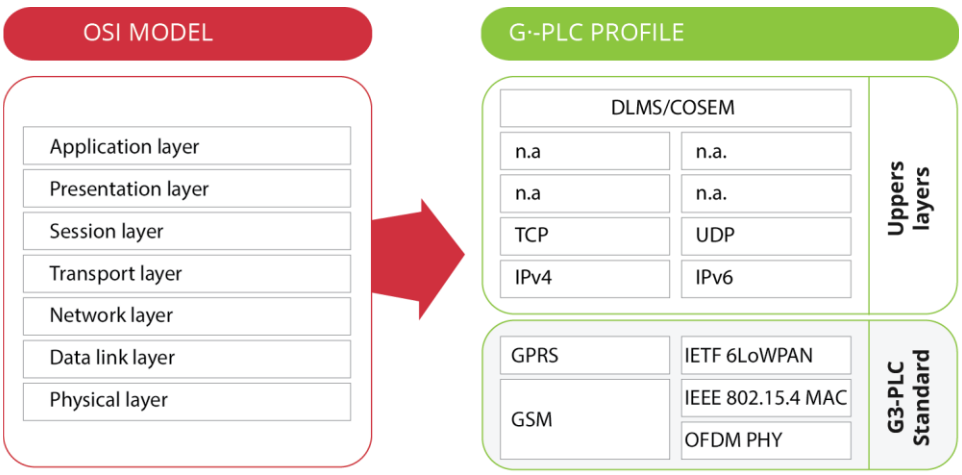

Figure 6. Sample of G3-PLC protocol and the OSI model

The encapsulation of the data of the G3-PLC protocol, through the different layers with presence of this protocol are summarised in Figure 7.

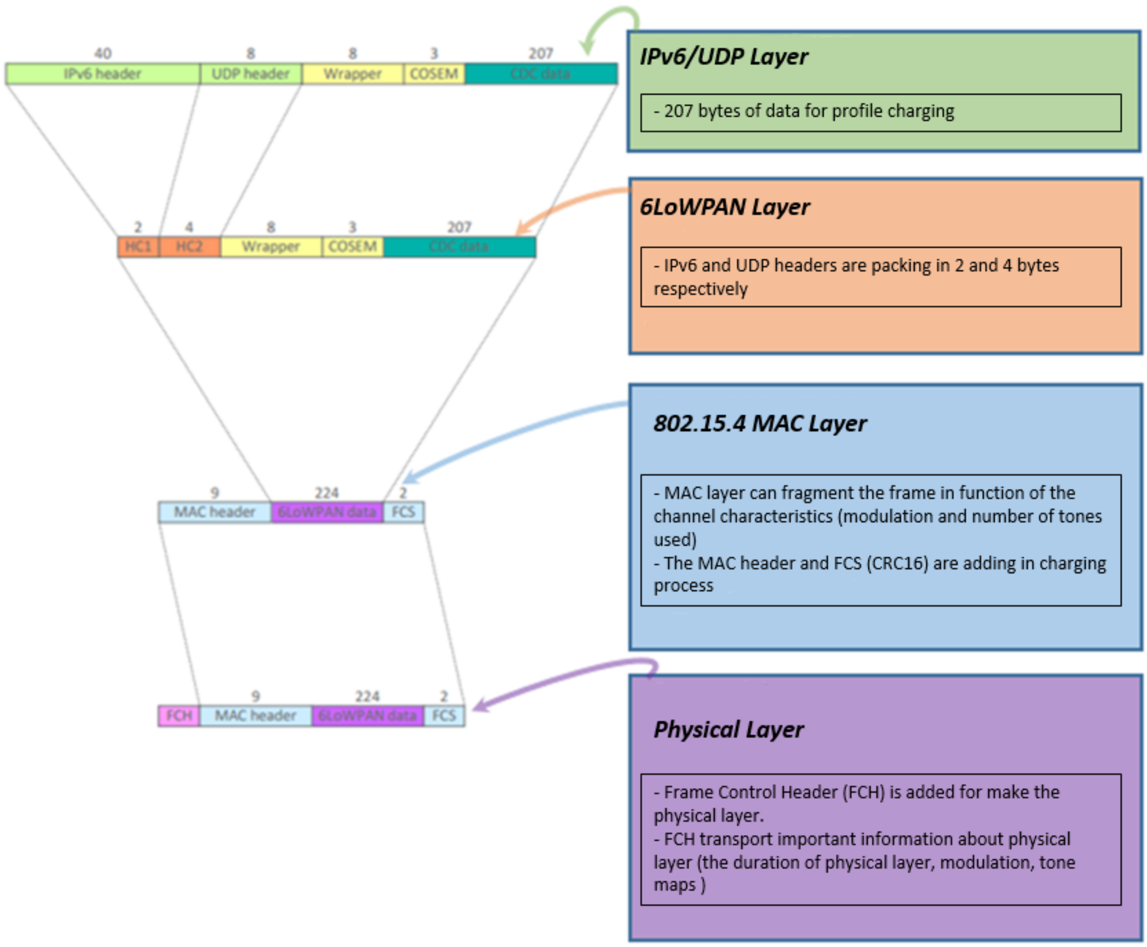

Figure 7. Route of data in the 3G-PLC protocol

The map in Figure 8 shows the countries currently using the G3-PLC protocol and the bodies that regulate the frequencies that can work with devices that implement this protocol in each area. By the year 2018, it is forecast that 35 million devices will be deployed using this protocol in France alone.

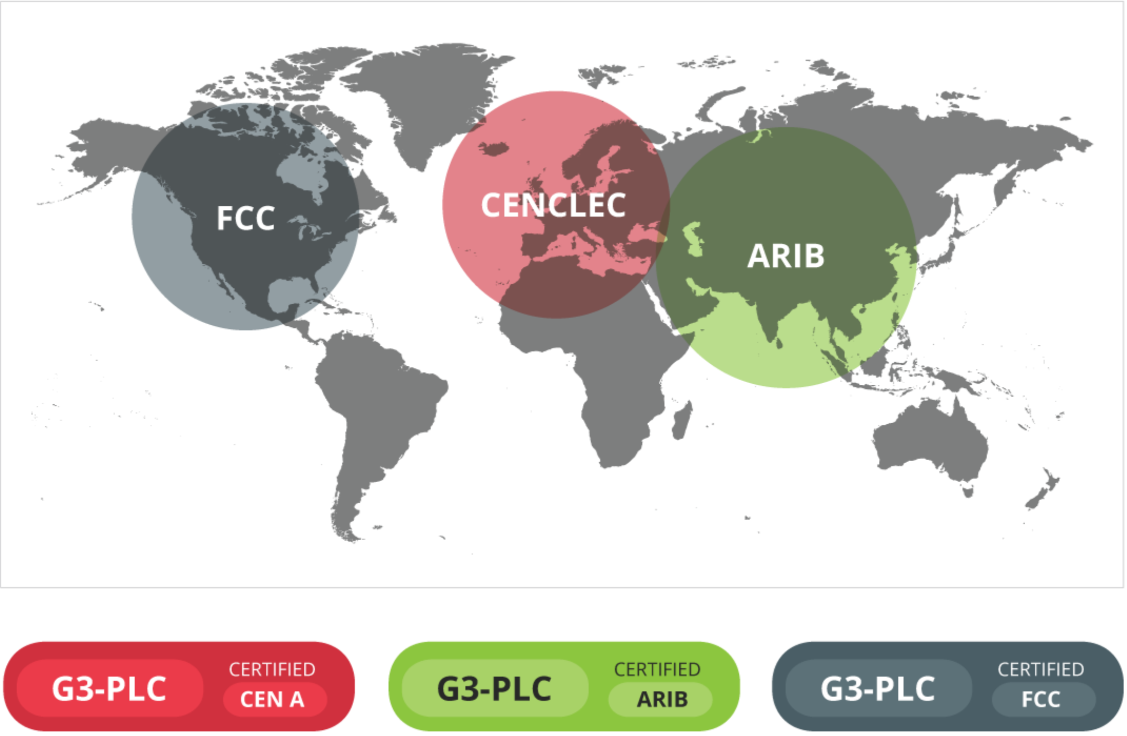

Figure 8. Areas where the G3-PLC protocol is used. Source: [G3-PLC Alliance]

4.3.2. Security

The G3-PLC method adopted for the implementation of security at physical level by G3-PLC consists of AES-128 encryption at the level of media access control (MAC), equivalent to layer 2 of the OSI model, which has the following features:

- Simplicity: Based on a single credential (a 128 bits pre-shared key) and a single encryption algorithm (AES-128).
- Security: It has a well-known and improved design of cryptographic schemes.
- Extendibility: In the case of OFDM over PLC, it can be easily extended to support group key distribution.

Confidentiality and integrity are insured at MAC level. As defined in IEEE 802.15.4 a type of CCM[19] is delivered to each transmitted frame between the nodes of the network. The mode of CCM encryption is used in the MAC layer, and prevents unauthorised access to network devices that perform malicious actions in same and in other processes at lower layers. MAC frames are encrypted and decrypted at each hop. The only exceptions are some frames in the early stages of the start-up process[20]. To support this service, all network nodes receive the same group master key (GMK). This GMK is distributed individually and securely to each node through the EAP-PSK secure channel.

In addition, G3-PLC presents two different authentication architectures:

---

[19] The CCM provides encryption of data through a 128 bits key and a message authentication code (MAC) using packet signature mode.

[20] https://en.wikipedia.org/wiki/Bootstrapping

- The function of the authentication server is directly supported by an LBS (LoWPAN BootStrapping Server)[21]. In this case all the authentication material (credentials, access lists, etc.) must be loaded to the LBS. The LBS contains the baseline information of each active device.
- The authentication server is supported by a remote AAA server (authentication, authorisation and accounting). In this case, the LBS is only responsible for the transmission of EAP messages to the AAA server through a standard AAA protocol such as RADIUS[22].

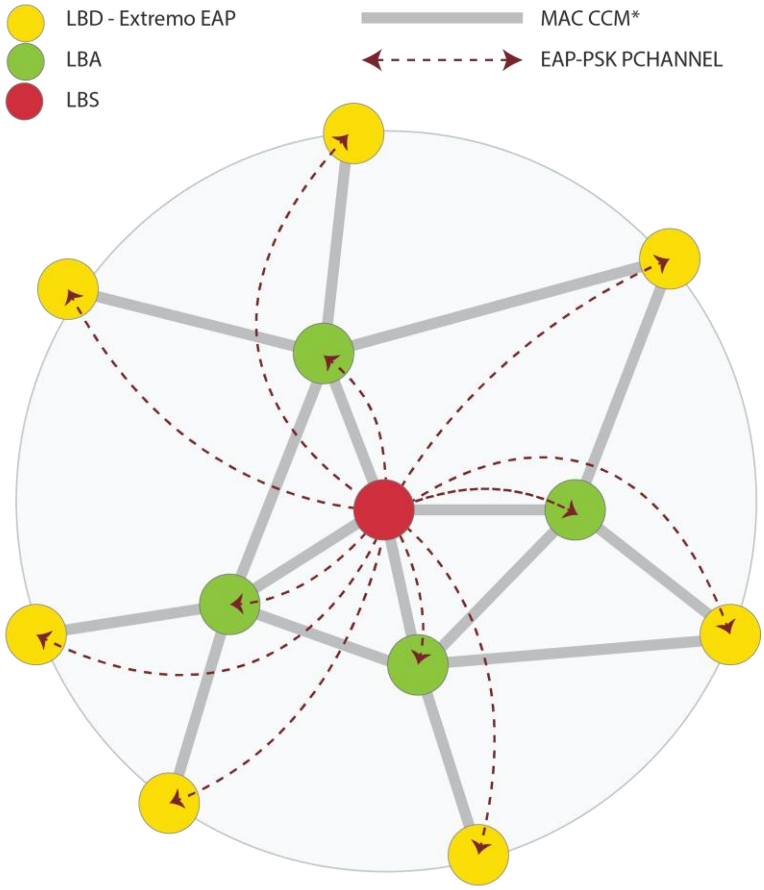

Figure 9. Confidentiality and security thanks the encrypted communication in G3-PLC. Source: Enedis

4.3.3. Security recommendations

As a communications protocol, G3-PLC does not avail of security options that can be enabled/disabled or configured according to needs. All measures are activated for use at all times. The only customisable option is the authentication, where it is recommended that the RADIUS protocol is used to establish authentication between the client and the AAA server.

Outside the protocol itself, it is recommended that there is correct filtering of information that arrives through the PLC networks.

[21] https://tools.ietf.org/html/draft-daniel-6lowpan-commissioning-02

[22] https://tools.ietf.org/html/rfc2865

As G3-PLC only implements the low levels of the OSI model, another product must be used for the higher levels. These higher level protocols must also have the security features available activated.

4.4. OSGP

4.4.1. Description

The Open Smart Grid Protocol (OSGP) currently applied in various countries on large scale Smart Metering projects. It was developed by OSGP Alliance[23] and published as a standard by the European Telecommunications Standards Institute (ETSI). It is one of the most used and tried protocols in the field of meters and smart networks and there are currently more than 100 million devices that support it across the world.

OSGP follows a modern focus based on the OSI model and the frequency at which devices that use it are found in a range between 9 kHz and 95 kHz. OSGP specifies an independent from media control layer for secure communication between meters and control nodes.

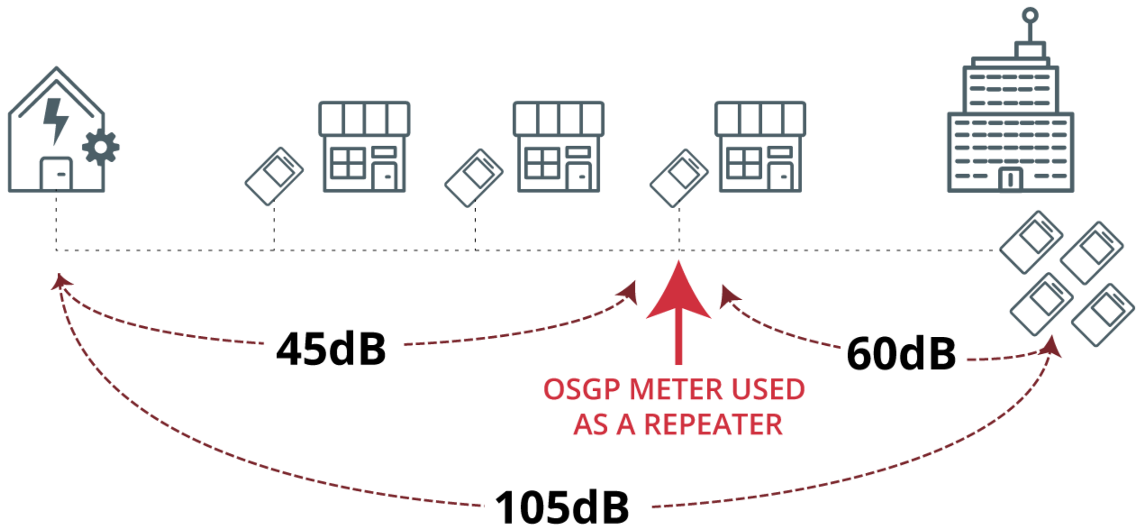

Figure 10. Intensities at which devices using the OSGP protocol operate Source: ESNA

OSGP is based on the following open standards:

- ETSI TS 104 001 (Application layer).
- ISO/IEC 14908-1 (Transport layer).
- ETSI TS 103 908 (Physical layer).

4.4.2. Security

The OSGP protocol requires the use of a mandatory transport security protocol called OSGP-AES-128-PSK, or OSGP-AES for short. This means it is not possible to disable security.

[23] http://www.osgp.org/

OSGP-AES provides a protected two-way communication channel between a client (e.g. a data concentrator) and a meter. The secure channel provides data confidentiality via AES-128-CCM encryption, data and origin integrity through authentication, and replay protection using sequence numbers. OSGP-AES secures both unicast and broadcast messages.

All OSGP messages are sent within the secure channel established by OSGP-AES. This includes reading personal meter data, such as energy consumption, as well as security critical functions, like changing the configuration of the meter. There are no exceptions, all communications are protected, and all messages exchanged are therefore subject to encryption, mutual authentication, and replay protection. This is in contrast to DLMS and other standards that allow security properties to be disabled or lowered, which results in insecure configurations.

OSGP-AES is designed to a use device-unique keys. This means that if one meter’s key is compromised, other meter keys remain secure.

OSGP-AES is specifically designed for constrained networks of legacy low-end embedded devices. Its primary use case is for Power Line Communication (PLC) networks. It is therefore able to provide high performance, while maintaining security.

Just like the rest of OSGP, the specification of the OSGP-AES security protocol is open, standardized, and can be freely accessed. The OSGP-AES security protocol was subject to an independent third-party review by a security expert. This report, which can be requested by contacting the OSGP Alliance, concluded:

“Overall, the protocol is secure, well designed and based on established cryptographic primitives (AES, CMAC and CCM) with reasonable parameters. These cryptographic primitives are used in ways that should not give rise to currently known attacks.”

The OSGP protocol also includes an older legacy security protocol called OSGP-RC4.

However, in 2015, the OSGP Alliance officially marked the OSGP-RC4 as deprecated, since it contained a number of security issues.

4.4.3. Security recommendations

The OSGP Alliance recommends to always use OSGP-AES as the OSGP security protocol. OSGP-AES has the same hardware and network resource requirements and has comparable communication performance to the deprecated older security protocol. In fact, OSGP-AES is actually faster in some cases, which means there is no performance limitation for using OSGP-AES.

All cryptographic primitives used by OSGP are standardized and approved for use by standards organizations including the National Institute for Standards and Technology (NIST). Specifically, OSGP-AES uses the following cryptographic primitives:

- AES-128: the 128-bit key variant of the FIPS-approved symmetric block cipher algorithm as specified in FIPS PUB 197.
- CCM: counter with CBC-MAC (CCM) as specified in NIST Special Publication 800-38C.
- CMAC: cipher-based Message Authentication Code (CMAC) as specified in NIST Special Publication 800-38B.

Since it is impossible to disable security, it ensures confidence that encryption and authentication provide the privacy and security protection needed for smart grid communications.

4.5. DLMS/COSEM

4.5.1. Description

DLMS/COSEM[24] is an application level protocol that defines from layer 4 to layer 7 of the OSI model. The initials that give their name to the protocol stand for the following:

- DLMS: "*Device Language Message Specification*", a generalised concept for an abstract model of communication entities.
- COSEM: "*COmpanion Specification for Energy Metering*", sets the rules, based on standards, for the exchange of information with energy meters.

This protocol is regulated by the standard IEC 62056[25].

Figure 11. Model of DLMS/COSEM layers

The DLMS/COSEM protocol was developed to be used jointly with the PRIME protocol, which operates on the lower levels of the OSI model and on network level protocols (IPv4/IPv6). Thus, communication is permitted with low level devices, such as smart meters, and communication with systems with more resources, such as the control centre equipment. There is also the possibility of using this protocol jointly with "Meters and More" protocol.

[24] http://www.dlms.com/

[25] http://www.dlms.com/documentation/dlmscosemspecification/iecstandardsforelectricitymetering.html

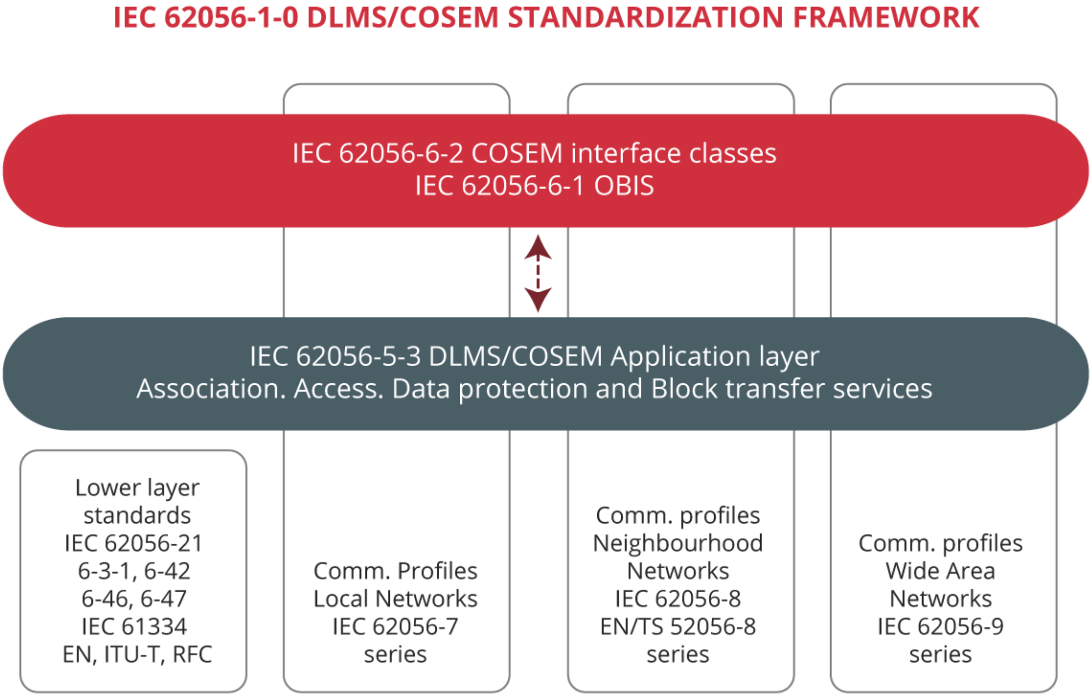

Figure 12. DLMS/COSEM architecture. Source: DLMS

4.5.2. Security

The security of the DLMS/COSEM protocol is divided across three different security levels:

- *Lowest level security*: This level provides no type of security to DLMS/COSEM communication.
- *Low Level security*: The security of the DLMS/COSEM communication is based on the use of credentials. The customer is provided with a password in order to carry out communication.
- *High Level security*: This is the maximum security level permitted. The client and the server must carry out a mutual authentication method using a four-step process.

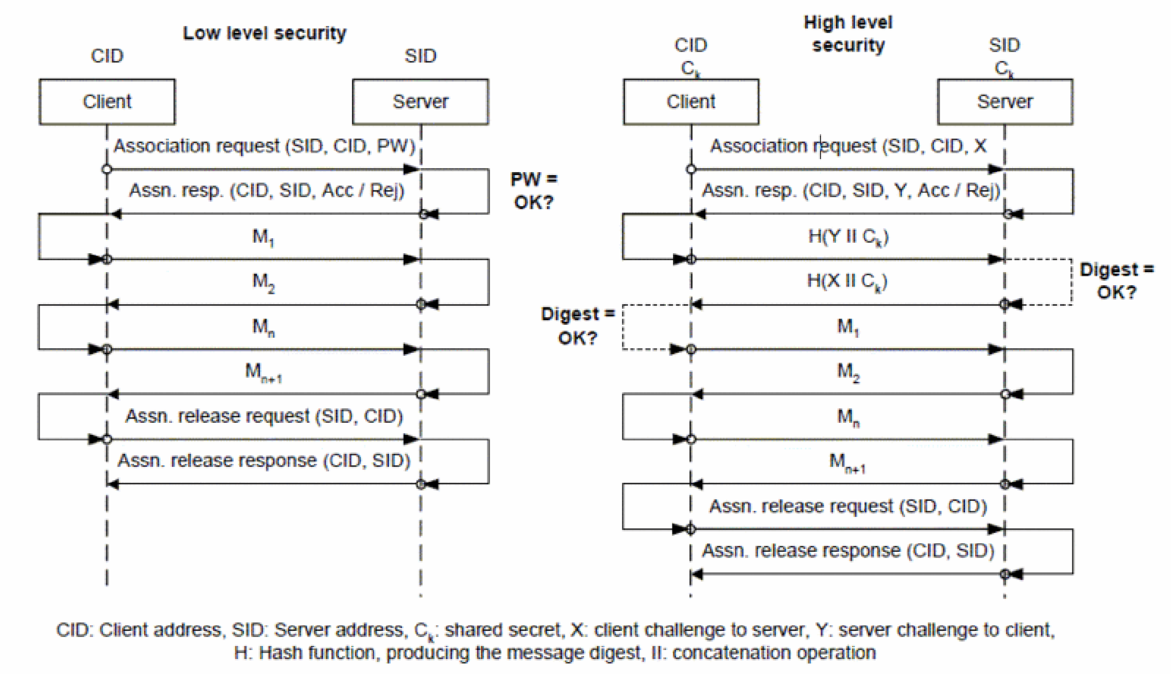

Figure 13. DLMS/COSEM authentication

The security context defines relevant security attributes for cryptographic transformations and includes the following elements:

- Security suite: Determines the algorithm used and use of encryption (AES 128).
- Security policy: Determines the type of protection applied to protocol packets.
- Security equipment: Relevant information for the security algorithm, including security keys, initialization vectors, public key certificates, etc. Security material is specific to each algorithm.

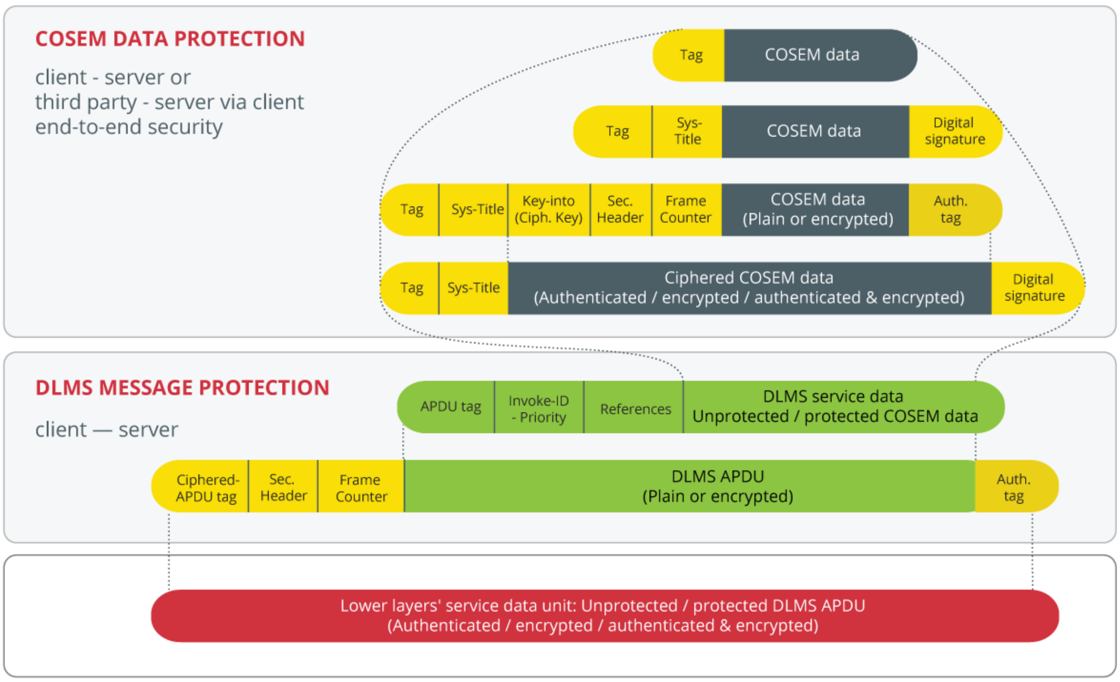

Figure 14. Security in DLMS/COSEM packets. Source: DLMS

4.5.3. Security recommendations

The DLMS/COSEM is a high level protocol with a presence in the application layer. This allows use of other protocols to reinforce security in lower layers were data transport occurs (encrypted), which in turn provides an extra level of security not present in other protocols. Moreover, it can use different protocols on the lower level, which may or may not have some security functions enabled to protect the sending of information between the client and the server independently of the media used.

Where possible, it is recommended that the “High Level Security” profile is used: the highest level of security provided by the protocol. To add a greater level of security it is also recommended that digital certificates be used alongside a PKI infrastructure to carry out authentication of communication devices.

When DLMS/COSEM is used over TCP/IP, it is possible to use security communications tools such as firewalls and IDS/IPS devices. The default port used is 4059, which is why it is recommended the traffic associated with said port be monitored.

4.6. IEEE 1901

4.6.1. Description

The IEEE 1901-2010 standard defines a high-speed communication standard, up to 500 Mb/s in the physical layer, Broadband over Power Lines (BPL). This standard uses transmission frequencies below 100 MHz. All types of BPL devices can use this standard, including those used for connections within 1500 meters of the facilities to the Internet access services. The standard defines the physical (PHY) and link (MAC) layers.

The IEEE 1901 standard can include two different physical layers, both based on Orthogonal Frequency-Division Multiplexing (OFDM): one is FFT (Fast Fourier Transform) OFDM, and the other is Wavelet OFDM. Each physical layer is optional, so it is not mandatory to implement both specifications simultaneously. FFT is derived from HomePlug AV technology and is implemented in HomePlug-based products, while Wavelet is derived from HD-PLC (High Definition - Power Line Communication) technology and is implemented in products based on this technology.

In the FFT OFDM model, which allows data exchange at speeds of up to 400 Mbps with bandwidths of up to 50 MHz, it is necessary to have a guard interval to ensure that the different transmissions do not interfere, and thus manage to maintain orthogonality and redundancy. Optimal signal rectification is thus achieved in the transmission.

Wavelet OFDM technology provides efficient transmission and can coexist with existing systems (shortwave and amateur radio emissions). The speed of the physical layer is approximately 240 Mbps and is reached with a bandwidth of 26 MHz. In addition, high quality and reliable communications are achieved, even in domestic power transmission routes, where the physical medium is of poor quality, using solid error correction coding and a diversity mode.

In general, both FFT and Wavelet are very similar in their features, except for some points:

- Access priority, where Wavelet has the highest priority.

- In security, FFT can use DSNA/RSNA (Device-based Security Network Association / Robust Security Network Association) while Wavelet uses PSNA/RSNA (Peer Security Network Association / Robust Security Network Association).
- Burst mode operations can be unidirectional or bidirectional in FFT, while Wavelet does not support it.
- They use multiple access by carrier detection and collision prevention (CSMA/CA, *Carrier Sense Multiple Access with Collision Avoidance*) as a basic containment schema. It is also possible to use *Time Division Multiple Access* (TDMA) as a free containment schema.

Feature and technology		IEEE 1901	
		FFT-PHY	Wavelet-PHY
Channel access	Fundamental technology	CSMA/CA	
	Contention-based scheme	CSMA/CA	
	Access priorities	4	8
	Virtual carrier sensing	Yes	
	Contention-free scheme	TDMA	
	Persistent access	Yes	
	Access administration	Beacon based	
Security	Security framework	DNSA/RSNA	PNSA/RSNA
	Encryption protocol	CCMP	
Burst mode operation	Burst mode operation	Uni/bidirectional	Not supported
Addressing scheme	Modes	Unicast, multicast and broadcast	
	Space (per domain)	8-bit	
Framing	Aggregation, fragmentation and reassembly	Supported	

Figure 15. Comparison between the two physical layer versions of IEEE 1901. Source: [ResearchGate]

4.6.2. Security

At the security level, the IEEE 1901 protocol has the following characteristics within the link layer:

- Encryption using 128-bit AES keys.
- End-to-end protection.
- Access control.

The IEEE 1901 standard uses the security framework in IEEE 802.1X, together with the CCMP protocol (MAC encryption block chaining in counter mode). The IEEE 1901 working group was based on the 802.11[26] standard for wireless network security, which is based on the RSNA concept found in 802.1X and CCMP. The RSNA defines a series of security features:

- Enhanced authentication mechanisms for stations.
- A set of key management algorithms.
- Establishment of cryptographic keys.
- Enhanced cryptographic data encapsulation mechanism, called counter mode with CCMP.

[26] https://standards.ieee.org/standard/802_11-2016.html

4.6.3. Security recommendations

IEEE 1901 security is based on the IEEE 802.1X framework in general, using the IEEE 802.1i standard on security in wireless networks as the main foundation.

The IEEE 1901 standard incorporates security features in layer 2 of the OSI model, including encryption and authentication mechanisms, which should be used in all scenarios in which it is possible. It also implements a series of additional recommendations set out in several reports by the ITU (*International Telecommunication Union*), where several security tips are specified in layer 2 of the OSI model, such as encryption, authentication and key management procedures.

Moreover, as an additional protective measure, it uses the IEEE 802.11 security standard, which is specific for the physical and link layers. Thus, its security does not only depend on the IEEE 1901 protocol itself. The security features provided by IEEE 802.11 include authentication control and encryption or identification of devices on the network.

5. Comparison summary table

	Protocol	PRIME	DLMS/COSEM	Meters and More	G3-PLC	OSGP	IEEE 1901
General Aspects	Type of Standard	Open	Open	Proprietary	Open	Open	Open
	Transmission Media	PLC	Ethernet	PLC Ethernet Serial	PLC Ethernet	PLC Ethernet	PLC Ethernet
	Region of Use	Spain	Spain	Italy Spain	France	Northern Europe	Spain
	Compatibility	DLMS/COSEM	PRIME M&M G3-PLC OSGP	DLMS/COSEM	DLMS/COSEM	DLMS/COSEM G3-PLC	802.1X
Security	Encryption	Profiles 1 and 2	Low and High Levels	YES	YES	YES	YES
	Authentication	Profiles 1 and 2	Low and High Levels	YES	YES	YES	YES
Layers implemented by the protocol (OSI level)	1	X		X	X	X	X
	2	X		X	X	X	X
	3			X	X	X	
	4		X	X	X	X	
	5		X		X	X	
	6		X		X	X	
	7		X	X	X	X	
Security Recommendations		Use security profile 1 or 2	Use High Level security Over TCP/IP, perform filtering in port 4059	In joint deployments with DLMS/COSEM apply security in both protocols	Use authentication via RADIUS	Use OSGP-AES	Use IEEE 802.11 standard

Table 1: Table of summary of protocols in smart networks

incibe cert_

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD