International Journal of Engineering & Technology, 7 (3.34) (2018) 554-557

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Design Key Management System for DLMS/COSEM Standard-based Smart Metering

Seung-Hwan Ju[1], Hee-Suk Seo[1*]

[1]Dept. of Computer Engineering, Koreatech, Dongnam-gu, Cheonan-si, 31253, Republic of Korea
[*]Corresponding author E-mail: histone@koreatech.ac.kr

Abstract

Background/Objectives: Security features are an essential part of recent smart metering systems. Smart meters are considered an important facility that must be protected by applying the latest security technologies.
Methods/Statistical analysis: Security context determines the rules for applying/verifying security. DLMS/COSEM have Security suite to set of cryptographic algorithms. This is based on symmetric key based cryptographic communication. The high level security requires public key based cryptographic communication and digital signature.The security specification references the key scheme of DLMS-COSEM, which is based on a single set of unique symmetric keys per meter.
Findings: we have studied a sequence for distributing security keys required by DLMS / COSEM.
Our smart metering key distribution system can provide a security key management system such as key generation / distribution between AMI components. This is a PKI-based authentication using public key method (ECC), and a DLMS standard key distribution method after generating a session key using a public key. This system can also provide a key management scheme between DLMS clients not defined in the DLMS standard.
Improvements/Applications: we analyze security requirements of DLMS/COSEM for secure smart metering and design key distribution/management method.

Keywords: *Smart-Metering, Security, Key Distribution, DLMS/COSEM, IEC 62056, Security suite*

1. Introduction

Smart metering, which provides a key indicator of energy production, consumption and management, utilizes the latest information and communication technology (ICT) to digitize the traditional information technology and metering information to create energy new industries such as energy efficiency and demand management. The electricity market in the world is separated from the power transmission and distribution sector, and the power supply subject is also being liberalized and opened from the monopolistic fashion in the past [1]. Thus, it is complex and competitive in that various users consume various energy sources provided by various suppliers. Metering in this diverse environment requires selective and reliable data access, and it focused attention on interoperability issues. The DLMS /COSEM communication protocol based on IEC 62056 international standard is a current global issue as a communication protocol of intelligent metering[2]. In future, this protocol will apply not only to electricity, but also to gas and water, and it is gradually expanding and attention focused on standard protocol of smart metering. It is an electronic meter communication protocol for remote meter reading and is widely used throughout smart metering as it is established as IEC 62056 international standard and DLMS UA collective standard. It is necessary to become familiar with the terminology in order to understand the standard technology. COSEM is an energy object and can represent as an independent object that contains metering information (properties) and functions (methods) of energy. The COSEM defined in the DLMS/COSEM standard has the following information:

① Data storage for weighing information
② Access control and management
③ Time and event related control
④ Payment

DLMS defines application commands for access (Read/Write) of energy objects defined by COSEM and functions using various communication media such as PLC (Line Communication) and RF-Mesh [3]. This is similar to the language we use, and even if we use a variety of communication media such as the Internet, messenger, and telephone, the language used to exchange information can understand to be the same. When referring to data objects using DLMS, the OBIS is used as an identifier to identify these objects.
The smart metering system requires various functions such as metering, access control, management and data exchange in various communication media. For flexibility and scalability of such a smart metering system, DLMS/COSEM has the following modeling – messaging - transport. It defines the architecture [3-5].
Modeling: The COSEM object model and the OBIS object recognition system model the functions of the meter that can view within their interface. This model includes a set of procedures in which all energy types and messages are designed and transmitted. The contents are described in IEC 62056-61, 62 and the DLMS-UA Blue Book.
Modeling: The COSEM object model and the OBIS object recognition system model the functions of the meter that can be viewed within their interface. This model includes a set of procedures in which all energy types and messages are designed and transmitted. The contents are described in IEC 62056-61, 62

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

and the DLMS-UA Blue Book.
Messaging: DLMS / COSEM Application layer protocol that specifies messages to access data modeled by COSEM objects. It is specified in IEC 62056-53, DLMS-UA Greenbook for lower layer protocols.
Transport: A communication profile that specifies how DLMS / COSEM is used in various standardized communication media. These are specified in the Greenbook which partially complies with IEC, CENELEC and CEN.
In order to operate a smart energy system safely, user authentication, device authentication, device-to-device communication protection, and infrastructure-level security that includes all of these are essential. The DLMS/COSEM is a symmetric key and a public key based cryptographic algorithm that provides authentication for user authentication and confidentiality and integrity as well as security key transmission through AES key WRAP, authentication for message integration and cryptanalysis respectively. In addition, the protection of the metering information in the environments using various communication methods depends on the data and level protected in the DLMS message and the COSEM data between the meter and the third party (third party) or the meter and the HES It is designed to be applied. The standard defines a mutual authentication method for accessing a logical device by a security function of a smart meter and access rights for a user or role for reading, writing or a method of attribute information of an energy data object in a logical device [6-8]. COSEM data objects used in projects that utilize smart meters standardize data from dozens to hundreds of times, metering, power quality, switch control, and communications. Access control divides energy objects logically into groups according to the user. We propose a model that protects and widely utilizes metering information by preventing unreasonable misuse of information by defining authentication methods and access control rules for energy objects and effectively providing appropriate data for each service through logical devices [8].
Security features, including object authentication for smart meters, access rights operations and message encryption, are essential parts of recent smart metering systems. Smart meters consider an important facility that must protected by applying the latest security technologies. In this paper, we analyze security requirements of DLMS/COSEM for secure smart metering and design key distribution/management method.

2. DLMS/COSEM Security

DLMS/COSEM has the following security requirements:
Authentication of communicating partners
Controlling access rights depending on the role of the client
End-to-end security between third party and server
Protection of COSEM data and xDLMS messages

Table 1: DLMS/COSEM security requirements [9]

Category	Requirements	Description
Access Security	Device mutual authentication	▪ LLS and HLS authentication
Transport Security	Message encryption Authentication	▪ AES128 / 256 based encryption ▪ Provide dedicated key encryption based on ECC KA
	Message Authentication Digital Signature	▪ ECC-based electronic signature support, non-repudiation support

There are two kinds of security like Table1. Access security concerns the rights of a client to access to data stored in a given server. Transport security concerns the 'ciphering' applied to the information exchanged between the server and the client [9-10].

2.1. Access Security

The interface class that defines the logical device applies Association LN. OBIS code of attribute 1st, 2rd is COSEM object for logical device, defines class ID, logical name, and access authority for object. In addition, the SAP information of the client accessing the LDN, so that the session can be managed in the current communication process. It contains a reference to the Security Setup interface class for implementing the security functions and the security mechanism that should implement when the application first connects for mutual authentication of the logical device [9-11]
The communication process for the logical device defined in this way is a three-step process as shown in Figure 1. Application Association is a process (COSEM-OPEN) for accessing energy data objects. This requires mutual authentication between the client and the server. The basic security concept is generated by generating mutual random numbers and re-exchanging the secret message generated through the cryptographic technique using the shared secret key between the counterparts of the random number. (HLS Authentication)
In the second step, the DLMS messages for information retrieval (Get), information writing (Set), and method execution (Action) mutually encrypt and combine in an encrypted manner for the energy object, Ensure confidentiality and integrity. Finally, after exchanging the message, AA release process is performed to end the session.
In COSEM, access security is implemented by Association Request / Association Response exchanges. Clients and servers are identified by addresses and negotiate authentication contexts. Members Mechanism Name of Association Request specifies
the level of security that clients use to access the server. Possible values are:

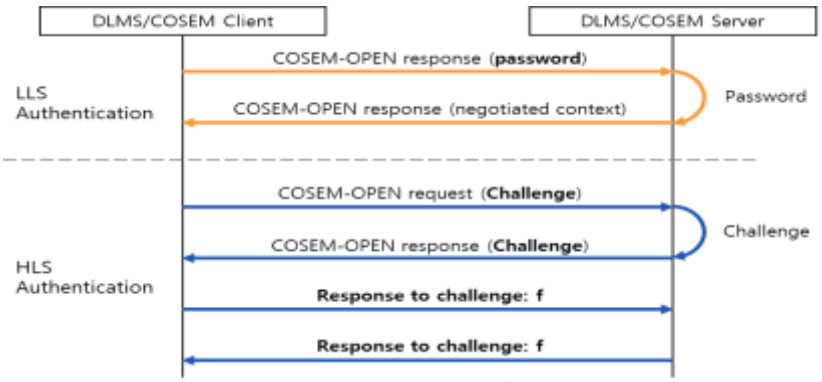

Figure 1: Authentication method of DLMS/COSEM

Lowest level security: this is in fact "no security" at all.
Low Level security: the client has to provide a valid password
High Level security: the client and the server have to identify themselves using a 4 passes process.

2.2. Transport Security

The xDLMS APDU carrying the service primitive can be password protected. The security context and access rights determine the required protection. To provide end-to-end security between third parties and servers, these third parties can use the client as a broker to access resources on the server. In addition, the COSEM data carried by the xDLMS APDU can be password protected [11].
The following functions are required for smart metering security:
Device mutual authentication
Message encryption / authentication
Establish a secure data communication channel
Security context determines the rules for applying/verifying security. DLMS/COSEM have Security suite [Table 2] to set of cryptographic algorithms.
This is based on symmetric key-based cryptographic communication, but high-level security requires public key based cryptographic communication and digital signature.
Transport security is performed using an encrypted COSEM service instead of a regular COSEM service. All generic COSEM services (ReadRequest, GetRequest, ReadResponse, WriteResponse, etc.) have a corresponding encrypted variant. The COSEM / DLMS symmetric key security system uses Gallois Counter Mode with the AES-128 algorithm. The encryption procedure has six inputs and delivers one output [11].The encrypted message is transmitted as shown in Table 3.

Table3: APDU Transport sequence

Sender	Receiver
1 - Convert the plain xml to APDU	-
2 - Cipher the APDU	-
3 - Create the glo_ service	-
4 - Convert to APDU and transmit using HDLC or WRAPPER	4 - Receive the response APDU
	5 - Convert to xml to have the glo_ service
-	6 - Extract the embedded ciphered frame
-	7 - Decipher to a GetResponse APDU
-	8 - Convert the plain APDU to xml

Table2: DLMS/COSEM Security Suites

Security Suite ID	Authenticated Encryption	Digital Signature	Key agreement	Hash	Key-transport
0	AES-GCM-128	-	-	-	AES-128 Key wrap
1	AES-GCM-128	ECDSA with P-256	ECDH with P-256	SHA-256	AES-128 Key wrap
2	AES-GCM-256	ECDSA with P-384	ECDH with P-384	SHA-384	AES-256 Key wrap

3. Certificate Management System

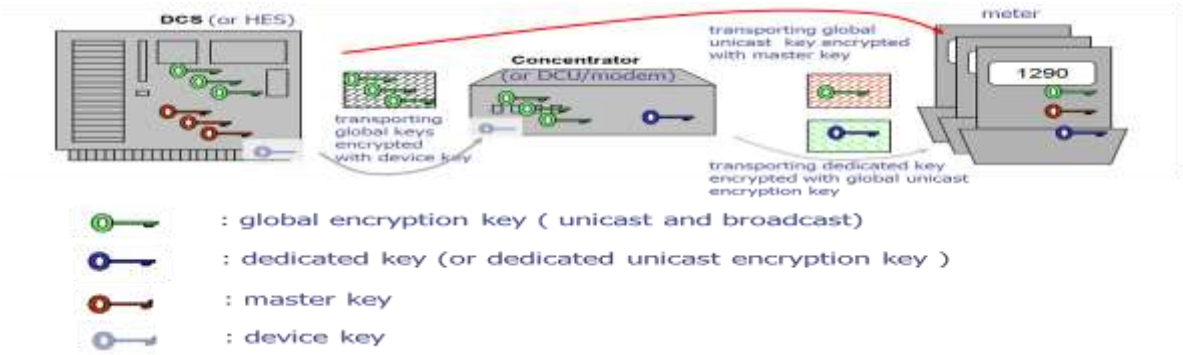

Figure 2: DLMS/COSEM example for manage of security keys

To satisfy the DLMS / COSEM Security of Chapter 2, we must have a public key-based authentication scheme. DLMS/COSEM Security requires a security keys [Table4]. In this study, we design a method and system for distributing it.

Table4: DLMS/COSEM Security key and their management

Key type	Purpose
Master Key, KEK	Key Encrypting Key(KEK) for : (new) Master key Global encryption or authentication keys Ephemeral encryption keys
Global unicast encryption, GUEK	Block cipher key for unicast xDLMS APDUs and/or COSEM data
(Global) Authentication key, GAK	Part of Association to the ciphering process of xDLMS APDUs and/or COSEM data
Dedicated key (unicast)	Block cipher key of unicast xDLMS APDUs, within and established Association
Ephemeral encryption key	Block cipher key for xDLMS APDUs and/or COSEM data

Many keys are used for secure smart metering communications. The key must be updatable and must be able to authenticate with other components using the new key. Therefore, a key management system is required, and it is expected that the key be transmitted securely and correctly. We designed key management service that is not defined in DLMS / COSEM to be compatible with DLMS/COSEM specification.
According to Figure 2, Master key identify as the KEK in general ciphering APDUs between client-server. Global keys (GUEK, GBEK) service-specific global ciphering APDU client-server. They are used object protection parameters. Encryption is the process of using an algorithm to transform information so that it is not read by anyone other than the owner of the key. Secure communications are imperative for data transfer between devices in the measurement, switching and display system and the components of data collection system, such as a data concentrator or the head end system. The DLMS-COSEM protocol provides several security features for data authentication and transport. Data transfer security provides privacy and authentication of data as it moves from multiple energy meter points to the next system instance.
The main steps in the smart metering security key-generation and management process are as follows like Figure 3:
Step 1: The manufacturing facility uses a secure key manager software and secure key storage hardware to generate an initial unique key set for each meter consisting of a master key (a key encryption key) and initial global keys (GUK, GBEK, and

GUEK).
Step 2: The global keys are encrypted using the master key and written to the meter.
Step 3: The KMS (Key management system) sends a copy of the key material to the utility AIM system using signed secure based on the public key infrastructure.
Step 4: The utility AIM system stores and manages the key material using its local secure key manager and secure key storage hardware.
Step 5: As each meter is registered to the AIM system as part of the installation process, AIM securely distributes the key material to appropriate data concentrator (using TLS over mobile communications) and initiates communication with the meter.
Step 6: As part of the communication initialization process, AIM renews the meter's global keys and distributes them to the data concentrator and meter.
Step 7: All communication from the head end system to the meter via the data collection system authenticated and encrypted using the renewed meter-specific keys.

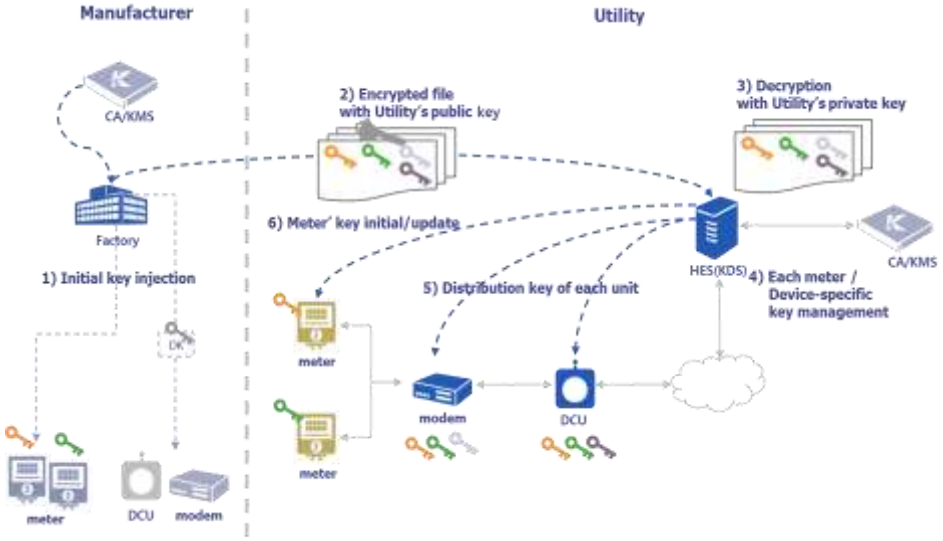

Figure 3: Design of Key distribute system for Smart metering

5. Conclusion

Smart metering technology can provide efficient energy saving through more reasonable energy consumption by providing various kinds of data, and it is expected that demand management and load distribution will be possible by energy resource. Smart metering is an energy management service based on two-way data communication. It supports a wide range of applications such as remote meter reading, customer relationship management and demand-side management. Smart metering provides utilities support for load control, power failure reporting, and power quality monitoring.
DLMS/COSEM specifies security functions such as encryption, authentication, and digital signature. To build this security function, the key management system is needed. We designed a key management system that not define in the DLMS standard
Our smart metering key distribution system can provide a security key management system such as key generation / distribution between AMI components. This is a PKI-based authentication using public key method (ECC), and a DLMS standard key distribution method after generating a session key using a public key. This system can also provide a key management scheme between DLMS clients not defined in the DLMS standard.

Acknowledgment

This paper was partially supported by the Education and Research Promotion Program

References

[1] Darby, S. (2010). Smart metering: what potential for householder engagement. Building Research & Information, 38(5), 442-457.DLMS User Association. (2007). DLMS/COSEM. Architecture and Protocols.
[2] Jain, S., Kumar, V., Paventhan, A., Chinnaiyan, V. K., Arnachalam, V., & Pradish, M. (2014, March). Survey on smart grid technologies-smart metering, IoT and EMS. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on (pp. 1-6). IEEE.
[3] Schneps-Schneppe, M., Maximenko, A., Namiot, D., & Malov, D. (2012, October). Wired Smart Home: energy metering, security, and emergency issues. In Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on (pp. 405-410). IEEE.
[4] Zaballos, A., Vallejo, A., Majoral, M., & Selga, J. M. (2009). Survey and performance comparison of AMR over PLC standards. IEEE transactions on power delivery, 24(2), 604-613.
[5] Feuerhahn, S., Zillgith, M., Wittwer, C., & Wietfeld, C. (2011, October). Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications. In Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on (pp. 410-415). IEEE.
[6] Štruklec, G., & Maršić, J. (2011, May). Implementing DLMS/COSEM in smart meters. In Energy Market (EEM), 2011 8th International Conference on the European (pp. 747-752). IEEE.
[7] Kmethy, G. (2009). IEC 62056 DLMS/COSEM workshop. Part 5: COSEM data model. Metering Europe, Vienna.
[8] Ju, S. H., Park, Y. I., Sim, S. G., Lim, M. C., Han, S. H., & Seo, H. S. (2016). Meter-HES mutual authentication in the smart grid AMI environment. International Journal of Security and Its Applications, 10(12), 43-52.
[9] Weith, L. (2014). DLMS/COSEM protocol security evaluation.
[10] Kim, S., Chng, H., & Shon, T. (2014, November). Survey on security techniques for AMI metering system. In SoC Design Conference (ISOCC), 2014 International (pp. 192-193). IEEE.
[11] McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. IEEE Security & Privacy, 7(3).