THE PKI-BASED DEVICE AUTHENTICATION SYSTEM FOR AMI

Taehun Kim
KEPCO KDN – Korea
thkim@kdn.com

Muyong Hyun
KEPCO KDN – Korea
myhyun@kdn.com

Jaehee Kim
KEPCO KDN – Korea
byerain@kdn.com

Jincheol Kim
KEPCO KDN – Korea
kjc@kdn.com

Jonghwa Kim
KEPCO KDN – Korea
kimjh@kdn.com

Donghoon Lee
KOREA UNIVERSITY – Korea
donghlee@korea.ac.kr

ABSTRACT

As the power grid converges with ICT to evolve into a smart grid, various services such as AMI have been introduced. However, it has also inherited all of the security threats of the existing ICT environment, and thus attacks against it can cause leaks of device information and other types of serious damage to the network. This paper proposes a PKI-based device authentication system which is differentiated from existing PKI authentication and well optimized for smart grid device environment to develop a safe and reliable network environment between devices authorized through the legal authentication process and the server, and then applies it to the AMI environment.

INTRODUCTION

The smart grid is the next-generation power network which combines the existing power network with Information and Communications Technology (ICT) to optimize energy efficiency through bi-directional and real-time communication between suppliers and consumers. It can encourage rational energy consumption through bi-directional power information interchange and provide high-quality energy and value-added services. It can also create new businesses through the combination and expansion of clean green technologies such as renewable energy and electric vehicles. Currently, various technologies for the smart grid are being studied as a part of the efforts to cope with global climate change.

One of the key smart grid technologies is advanced metering infrastructure(AMI) which enables the introduction of various rating systems and the effective management of fault information based on remote metering data. As both smart grid and AMI technologies used for the optimization of power usage combine ICT with the power network, and thus inherit the existing security threats of ICT, security has become an important issue. Since smart grid devices are scattered over a wide space, an attacker can easily access them and cause network problems, as well as tamper with important data in the network. Moreover, without an encryption and legal authentication procedure among communication objects, attacks can cause not only device information leakage but also critical damage to the entire smart grid network. Therefore, the development of a safe communication environment between devices authorized through the legal authentication process and the server is essential and application PKI technology based on certificate is necessary. Smart grid device environment is different from existing pc-based user authentication environment and lightweight cryptographic algorithm must be used and considered a high volume of certificate issuance and verification. And also not only certificate profile suitable for device but optimized procedures for device authentication structure is needed. This paper proposes a PKI-based device authentication system to develop a reliable device authentication environment and applies it to AMI.

This paper is organized as follows: At first, analyzes AMI and security threats, which is the background of proposed technology, and PKI researches related to smart grid. The second, defines the PKI system and AMI security requirements for device authentication. The third, describes the procedure optimized to device authentication and the next, implements and applies of the device authentication system to AMI; and, lastly, presents the conclusion.

BACKGROUND AND RELATED WORKS

This section describes AMI, application target of proposed system, and security threats and analyzes PKI researches related to smart grid.

AMI and security threats

AMI is both an infrastructure used for bi-directional information interchange between energy suppliers and users to efficiently manage energy resources and reduce energy consumption, and a system for the measurement, collection, storage, analysis and utilization of energy usage data. In terms of collaboration, it is the infrastructure by which a utility business acquires energy usage data and bills it.

AMI is vulnerable to various security threats such as DDoS attacks through malicious code infection, exposure of personal information, and tampering with billing data[1]. The DDoS attack targets the billing server, which

collects a large volume of power usage data, portal, meter data management system (MDMS) and other key servers of the AMI. Secondary attacks such as DDoS, exposure of personal information, and tampering with billing data can be made by hacking the main devices of HAN, such as tempering of firmware upgrades of smart devices, attacking the built-in vulnerabilities of smart devices, and physical attacks. Moreover, billing data bomb exploiting communication vulnerability, damage from billing data transfer, and incorrect demand data can cause instability in the power system or even large-scale power interruptions. Secondary attacks such as the hacking of smart meters can also lead to malfunction. For example, a malicious code can be inserted during an F/W upgrade of smart meters in order to cause a PDoS (Permanent DoS) and destroy digital devices. As the PDoS attack is embedded software, it is very difficult to detect and treat it or track the attacker using a vaccine program. Moreover, the device can be infected with malicious code by exploiting the built-in vulnerabilities of the smart meter.

Therefore, device authentication and encrypted communication are needed to create a safe AMI operating environment under various security threats.

Related Works

Numerous study applying and considering PKI technology for smart grid has been researched. Rajiv . K. Bhatia[2] indicated that trustful operation environment need to be developed for smart grid, which is two way communication technology, in order to secure smart grid and protect personal information and PKI technology is appropriate for defending against cyber attack. Smart grid devices should be authenticated and authorized through strong lightweight authentication mechanism. Also Seth Bromberger[3] described common problem associated with large-scale deployment of PKI technology in two sets of emerging and legacy technologies used within the smart grid, AMI and ICS networks. Vasudev Dehalwar[4] proposed multi-agent based PKI technology for smart grid to authenticate devices participating micro grid and each agent utilize information exchanges from neighboring agents to construct knowledge base that can be used in making efficient decision support system. Todd Baumeister[5] defined smart grid security requirements since unique requirements of the electrical power grid don't fit well into an existing PKI solution. and evaluated current PKI trust models, recommending adaptation toward a smart grid PKI that will meet the smart grid cyber security needs. Lastly, Anthony R. Metke[6] defined security requirements for the smart grid and proposed the application of PKI solution and trusted computing technique to smart grid technologies as a study on the security of the network based on the defined security requirements. Thus, the researches of applying PKI technology in a variety of smart grid security research has been studied

REQUIREMENTS

This section defines the AMI security and PKI system requirements for deploying the device authentication technology.

AMI Security Requirements

All AMI communications must be protected from cyber-attacks such as unauthorized wiretapping and tampering as well as being guaranteed end-to-end security. As such, the AMI system must provide security services that ensure confidentiality, data integrity, authentication, access control, availability, non-repudiation and key management.

First, the confidentiality of data transferred over the network and data stored in the system and devices in the AMI must be assured. Second, the integrity of data transferred over the network and data stored in the system and devices in the AMI must be assured. Third, mutual authentication between communicating objects must be assured during network communication in the AMI. For that, the smart meter interfacing the utility domain, smart utility network (SUN) domain and user domain of the AMI, as well as the utility interface system, must be certified by a certification center. Fourth, the AMI must perform access control, which assigns only the minimum privilege to an authorized member when a member of the AMI attempts to access another system or device of the AMI. Fifth, the availability of all networks and services must be assured. Sixth, the non-repudiation service must be provided when billing and demand response data are interfaced over the AMI. Seventh, the encryption key used for AMI information protection must be generated, distributed, stored and disposed of in accordance with safe and legal procedures. The encryption key and certificate owned by each member must be safely managed by the relevant security policy.

PKI System Requirements

Many organizations including National Institute of Standards and Technology(NIST), IEC and IEEE are conducting studies on open architecture-based smart grid security[7][8]. Unlike the conventional public certification system, PKI in the smart grid environment has many requirements and constraints. Since a smart grid device is cheap and has low functionality, it cannot use the encryption algorithm which requires high calculation performance, and the smart grid must enable requests for the authentication and verification of many devices. Moreover, there is an entropy-related issue in that devices do not have sufficient resources to generate a random number to induce the key, and there is a need to systematically manage the increasing size of the Certificate Revocation List (CRL) as the expiry period has extended, since the expiry period of the device certificate is relatively longer than certificates for

conventional systems. Considerations related to certificate status include the fact that certificates issued by manufacturers must contain information on the manufacturer, model and serial number of the device, and that the certificate must be able to confirm that the firmware of the device has not been tampered with, in addition to confirming the identification and verification of authentication information. In addition, the NIST algorithm and key length approved and recommended as safe by the FIPS should be used for the encryption technology[8]. A technology for coping with physical violations of important information such as the key should also be considered.

THE PKI-BASED DEVICE AUTHENTICATION SYSTEM

This section analyses objects flow consist of smart grid authentication environment and describes the optimized PKI device authentication procedure and implementation of the PKI-based device authentication system, and then applies it to the AMI environment.

PKI Device Certification Procedure

[Figure 1] shows the procedure for the PKI-based authentication of AMI devices. The device security system consists of the PKI certifying agency, device manufacturer, and AMI security service.

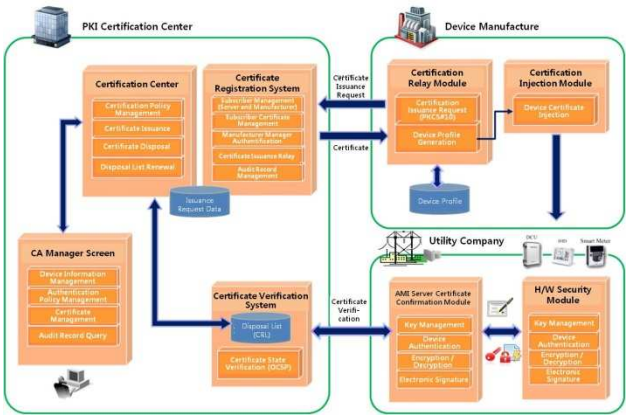

Figure 1. PKI Device Authentication Procedure

The PKI certification center consists of CA, RA, LRA and OCSP. It manages the authentication policy, issues and disposes of certificates, renews the CRL, manages subscribers, relays certification issuance, and verifies certificate status. The device manufacturer consists of a certificate relay module and a certificate injection module. It performs the function of certificate issuance request, device certificate profile generation, and device certificate injection. The AMI security service is the security function executed as part of smart grid application service. It consists of a server side security authentication module and a device side security authentication module. The AMI security service performs such functions as key management, device authentication, message encryption/decryption, and message electronic signature. The AMI security authentication procedure executes the following seven processes for device certificate generation, issuance and verification.

P1 <Device Certificate Request Form Generation Process>
(P1) The manufacturer generates the certificate request form based on the input data such as the device identifier and manufacturer identifier as well as PKCS#10.

P2 <Device Certificate Issuance Request Process>
(P2-1) The manufacturer requests the certificate of the smart grid devices through RA based on the PKCS#10 certificate request form.

(P2-2) RA verifies the validity of the received smart grid device certificate request forms and saves them in the request list.

P3 <Device Certificate Issuance Process>
(P3-1) CA regularly checks the list of PKCS#10 certificate request forms received and saved by RA, and issues the group of certificates and saves them in a specific location.

(P3-2) The saved device certificate is downloaded by the manufacturer through RA.

P4 <Device Certificate Disposal Process>
(P4-1) The manufacturer or RA accesses the LRA to request disposal of the certificate.

(P4-2) CA disposes of the requested certificate and renews CRL.

P5 <Certificate State Verification Process>
(P5-1) The AMI service server requests verification of the validity of the device certificate to the OCSP server at the certification center.

(P5-2) Upon receiving the request message from an AMI server, the OCSP server returns an OCSP response message containing the certificate status data.

P6 <Device Profile Generation Process>
(P6-1) The manufacturer verifies the certificate issued by CA.

(P6-2) The manufacturer generates the device profile with the device certificate, personal key, and CA certificate.

P7 <Device Certificate Injection Process>
(P7-1) The manufacturer loads the device profile to the device certificate injection module.

(P7-2) The manufacturer injects the device certificate through the device certificate injection module.

System Implementation

The PKI-based device authentication system consists of certificate issuance, registration, verification system, etc. The system was designed with consideration to the AMI device authentication procedure, low price/low specification, and high volume, and was implemented according to the relevant guideline and standard. The device certificate profile was defined and applied the X.509-based certificate standard containing the device data in the extended field and also derived certificate directory information tree structure fit to store device certificates, as well as an ECC encryption algorithm suitable for the RSA algorithm compatible device used for user authentication and delta CRL.

The certificate issuance system is mainly divided into the encryption/decryption engine and the certificate issuance server. It further consists of nine functions: the crypto engine related to encryption; key management engine related to the key pair; Oracle interface which defines the interface to the database; LDAP interface; certification issuance engine; revoked engine related to CRL/ARL; OPP interface managing the policy, audit and certificate; admin interface related to the administrator program; and communication related to the CTP engine. [Figure 2] shows the role of each function.

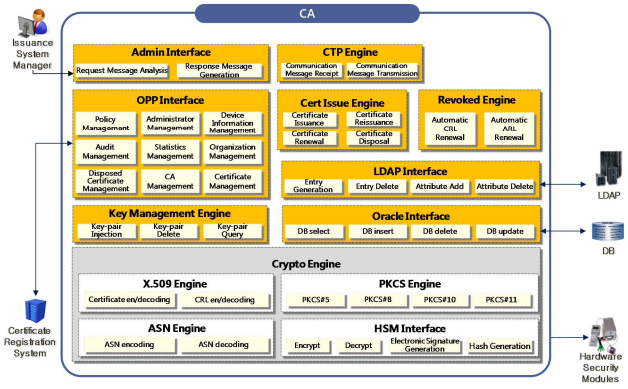

Figure 2. Certificate Issuance System Function Block Diagram

The certificate registration system is mainly divided into the certificate registration server and the encryption/decryption engine. It further consists of the six following functions: crypto engine related to encryption/decryption, Oracle interface which defines the interface to the database; OPP interface which manages the certificate registration system function; CA interface to communicate with the certificate issuance system; CTP engine for communication; and administration program providing the admin interface. [Figure 3] shows the role of each function.

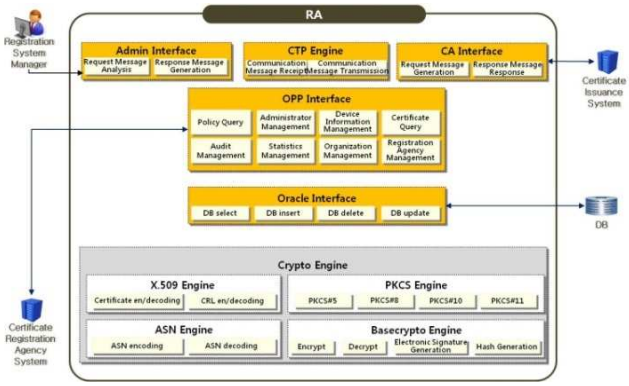

Figure 3. Certificate Registration System Functional Block Diagram

The certificate verification system is mainly divided into the certificate verification server and the AMI program API. It further consists of the following functions: crypto engine related to encryption/decryption; Oracle interface which defines the interface to the database; verify process engine to verify the certificate; verify interface to communicate with the business server; communication related CTP engine; and administration program related admin interface. [Figure 4] shows the role of each function.

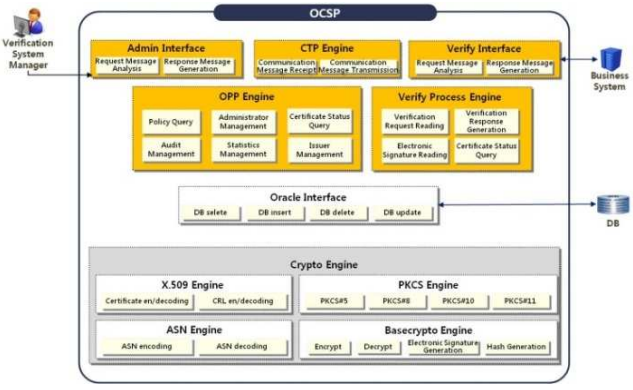

Figure 4. Certificate Verification System Functional Block Diagram

AMI Application and Test

The AMI security model shown in [Figure 5] was configured to apply and test the PKI-based AMI device authentication system.

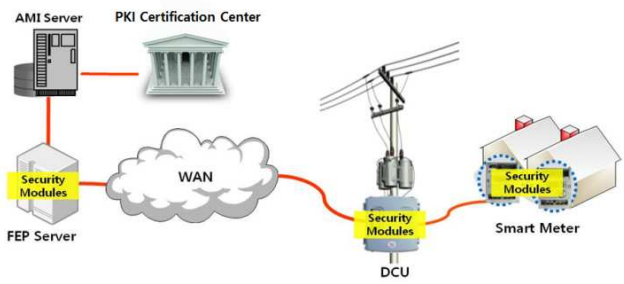

Figure 5. AMI Security Model

The AMI security model consists of a certification center, AMI server, FEP server DCU to balance the load, and smart meter. Each communication object has a hardware security module to safely keep the certificate and personal key, and calculates encryption at high speed. [Figure 6] shows the security processing procedure for operating the AMI.

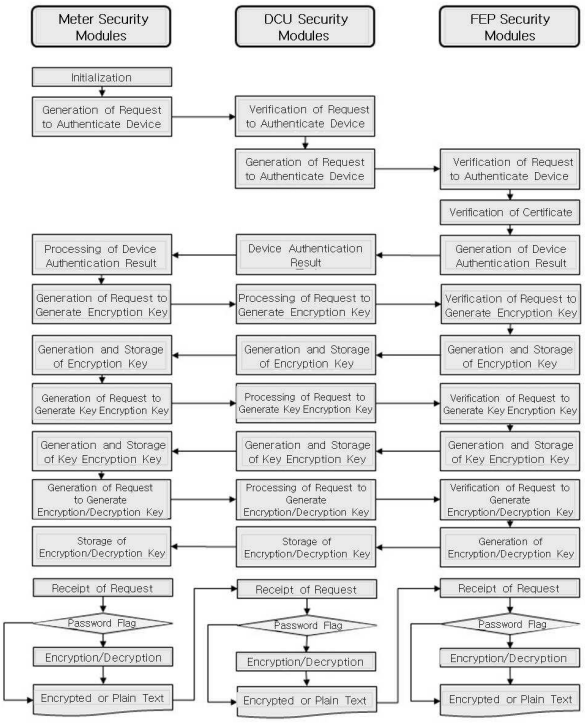

Figure 6. AMI Security Processing Procedure

The communication object shares the key and performs encrypted/decrypted communication after the mutual authentication procedure using the certificate issued by the device authentication system.

CONCLUSIONS

The smart grid, as the major next-generation power network, is set to replace the current power network and maximize efficiency by optimizing power usage. However, studies on the development of a safe communication environment are needed as the smart grid has inherited the security threats of existing ICT and thus is vulnerable to various attacks. As such, this paper proposes a novel PKI-based device authentication system optimized to smart grid device environment and applies it to the AMI in order to improve the security of AMI, which is the key smart grid technology. The PKI-based device authentication system proposed in this paper can be applied in all parts of the smart grid. We expect that a reliable smart grid device authentication system can be established by applying a safe authentication system and authentication policy in the future.

Acknowledgments

This work was supported by the Power Generation & Electricity Delivery Core Technology Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) granted financial resource (and received financial assistance) from the Ministry of Trade, Industry & Energy, Republic of Korea (No. 20121010500 04C)

REFERENCES

[1] Cleveland Frances M, 2008, "Cyber security issues for advanced metering infrastructure (AMI)." Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, IEEE

[2] Rajiv . K. Bhatia, Varsha Bodade, January 2014, “Smart Grid Security and Privacy: Challenges, Literature Survey and Issues”, International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE) Vol4, Issue1

[3] Seth Bromberger, Stan Pietrowicz, February 2012, “PKI Security Consideration for AMI, Smart Grid, and ICS Networks”, NESCO

[4] Dehalwar, Vasudev, R. K. Baghel, and M. Kolhe, 2012, "Multi-agent based public key infrastructure for smart grid", Computer Science & Education (ICCSE), 7th International Conference on. IEEE

[5] Baumeister Todd, 2011, "Adapting PKI for the smart grid" Smart Grid Communications (SmartGrid Comm), IEEE International Conference on

[6] A. Metke and R. Ekl, June 2010, “Security Technology for Smart Grid Networks,”IEEE Transactions on the Smart Grid, Vol. 1, No. 1, pp. 99-106

[7] NISTIR 7628 Revision 1, March 2013, “Guidelines on Smart Grid Cybersecurity: Vol. 1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements”

[8] NISTSP 800-57, March 2007, "Recommendation for Key Management"